# مجلة البحوث الإعلامية

مجلة علمية محكمة تصدر عن جامعة الأزهر/كلية الإعلام



**المراسلات:**

- القاهرة- مدينة نصر - جامعة الأزهر - كلية الإعلام - ت: ٠٢٢٥١٠٨٢٥٦
- الموقع الإلكتروني للمجلة: http://jsb.journals.ekb.eg
- البريد الإلكتروني: mediajournal2020@azhar.edu.eg

- العدد التاسع والستون- الجزء الأول - جمادى الآخر ١٤٤٥هـ - يناير ٢٠٢٤م
- رقم الإيداع بدار الكتب المصرية: ٦٥٥٥
- الترقيم الدولي للنسخة الإلكترونية: ٢٦٨٢ - ٢٩٢ x
- الترقيم الدولي للنسخة الورقية: ٩٢٩٧ - ١١١٠

## الهيئة الاستشارية للمجلة



## قواعد النشر

**تقوم المجلة بنشر البحوث والدراسات ومراجعات الكتب والتقارير والترجمات وفقًا للقواعد الآتية:**

- **يعتمد النشر على رأي اثنين من المحكمين المتخصصين في تحديد صلاحية المادة للنشر.**
- **ألا يكون البحث قد سبق نشره في أي مجلة علمية محكمة أو مؤتمرًا علميًا.**
- **لا يقل البحث عن خمسة آلاف كلمة ولا يزيد عن عشرة آلاف كلمة ... وفي حالة الزيادة يتحمل الباحث فروق تكلفة النشر.**
- **يجب ألا يزيد عنوان البحث (الرئيسي والفرعي) عن ٢٠ كلمة.**
- **يرسل مع كل بحث ملخص باللغة العربية وآخر باللغة الانجليزية لا يزيد عن ٢٥٠ كلمة.**
- **يزود الباحث المجلة بثلاث نسخ من البحث مطبوعة بالكمبيوتر .. ونسخة على CD، على أن يكتب اسم الباحث وعنوان بحثه على غلاف مستقل ويشار إلى المراجع والهوامش في المتن بأرقام وترد قائمتها في نهاية البحث لا في أسفل الصفحة.**
- **لا ترد الأبحاث المنشورة إلى أصحابها .... وتحتفظ المجلة بكافة حقوق النشر، ويلزم الحصول على موافقة كتابية قبل إعادة نشر مادة نشرت فيها.**
- **تنشر الأبحاث بأسبقية قبولها للنشر .**
- **ترد الأبحاث التي لا تقبل النشر لأصحابها.**

# محتويات العدد

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

«وقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ وَسَتُرَدُّونَ إِلَى عَالِمِ الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُمْ بِمَا كُنْتُمْ تَعْمَلُونَ»

سورة التوبة – الآية ١٠٥

# الافتتاحية

بقلم: الأستاذ الدكتور

**رضا عبد الواجد أمين**

رئيس التحرير

# مجلة البحوث الإعلامية .. ثلاثون عاما من الريادة والتميز

الحمد لله والصلاة والسلام على سيدنا رسول الله.

وبعد

أعزاءنا القراء من الباحثين والمهتمين بعلوم الإعلام والاتصال بفروعه المختلفة، نعتز بأن نقدم لكم العدد التاسع والستين من مجلة البحوث الإعلامية الصادرة عن كلية الإعلام جامعة الأزهر، والذي يصادف مرور ثلاثين عاما على إنشائها، حيث صدر العدد الأول منها عام ١٩٩٣م ، والتي نعتز فيها بإقامة جسور تواصل علمية مع نخبة من أكفأ الأساتذة الأفاضل في مجال التخصص لتحكيم وتنقيح البحوث العلمية والدراسات المجازة للنشر ، وصولا إلى الغاية المبتغاة ، وهي الارتقاء بالعملية البحثية ، وقيادة المجتمع العلمي للممارسات التي من شأنها الحفاظ على قوة ومكانة الدورية العلمية محليا وإقليميا وعالميا، مع التأكيد على أن عملية التحكيم تتم في جميع مراحلها عبر النظام الإلكتروني للمجلة، وأن البحث الواحد يحكم من قبل اثنين من الأساتذة في تخصص البحث بالنظام المعمى اتساقا مع المعايير العالمية في مراجعة البحوث والدراسات المعدة للنشر في الدوريات العلمية المرموقة.

وكم يسعدنا أن نتلقى ردود الفعل المثنية – من الباحثين – على الانضباط في كل عمليات التعامل مع البحث والباحث من المتابعة المستمرة ، وتجسير الهوة الزمنية بين تاريخ استقبال البحث وتاريخ نشره أو إجازته للنشر ، دون أن يؤثر ذلك على جودة كل المراحل التي يتم التعامل فيها مع البحث ، كما أن هناك نظام داخلي للتدقيق المستمر للتأكد من الشفافية والعدالة والموضوعية في كل بحث يتم الاتفاق على إجازته للنشر من قبل الأساتذة المحكمين.

وترجمة لهذه الثقة المطردة من قبل الباحثين والأساتذة فإننا يسرنا أن نعلن أن عدد قراءة الدراسات المنشورة في الموقع الإلكتروني للمجلة وهو : https://jsb.journals.ekb.eg/ زاد عن ٨٥٠ ألف قراءة ، وأن عدد تحميل البحوث Download بلغت ٩٢٠ ألفا وفقا لإحصائيات الموقع الإلكتروني في نهاية ديسمبر ٢٠٢٣م، وذلك بخلاف الاطلاع على النسخ الورقية في مكتبة كلية الإعلام جامعة الأزهر أو المكتبة المركزية بالجامعة أو أي وسيلة أخرى.

وهذا الأمر يضاعف من المسئوليات الملقاة على عاتق أسرة تحرير المجلة التي تعمل على المضي قدما في عمليات التحديث والتطوير ، في محاولة للإسهام الفاعل في البيئة العلمية والبحثية في تخصص مهم هو الإعلام والاتصال ، ونسأل الله أن يكون ذلك كله من باب العلم الذي ينتفع به ، و ندعوه سبحانه أن يجعل كل ما يتم من عمليات مستمرة في مجلة البحوث الإعلامية خدمة للباحثين والمهتمين في ميزان حسنات كل من له دور في ذلك ، وإنما التوفيق والعون من الله وحده ، فله- سبحانه- الحمد في الأولى والآخرة ، « وَمَا تَوْفِيقِي إِلَّا بِاللَّهِ عَلَيْهِ تَوَكَّلْتُ وَإِلَيْهِ أُنِيبُ»
(الآية رقم ٨٨ من سورة هود)

**أ.د/ رضا عبد الواجد أمين**

**عميد كلية الإعلام جامعة الأزهر**

**و رئيس التحرير**


| م | القطاع | اسم المجلة | اسم الجهه / الجامعة | ISSN-P | ISSN-O | السنه | نقاط المجله |
|---|---|---|---|---|---|---|---|
| 1 | الدراسات الإعلامية | المجلة العربية لبحوث الإعلام و الإتصال | جامعة الأهرام الكندية، كلية الاعلام | 2536-9393 | 2735-4008 | 2023 | 7 |
| 2 | الدراسات الإعلامية | المجلة العلمية لبحوث الإذاعة والتلفزيون | جامعة القاهرة، كلية الإعلام | 2356-914X | 2682-4663 | 2023 | 7 |
| 3 | الدراسات الإعلامية | المجلة العلمية لبحوث الإعلام و تكنولوجيا الإتصال | جامعة جنوب الوادي، كلية الإعلام | 2536-9237 | 2735-4326 | 2023 | 7 |
| 4 | الدراسات الإعلامية | المجلة العلمية لبحوث الصحافة | جامعة القاهرة، كلية الإعلام | 2356-9158 | 2682-4620 | 2023 | 7 |
| 5 | الدراسات الإعلامية | المجلة العلمية لبحوث العلاقات العامة والإعلان | جامعة القاهرة، كلية الإعلام | 2356-9131 | 2682-4671 | 2023 | 7 |
| 6 | الدراسات الإعلامية | المجلة المصرية لبحوث الإعلام | جامعة القاهرة، كلية الإعلام | 1110-5836 | 2682-4647 | 2023 | 7 |
| 7 | الدراسات الإعلامية | المجلة المصرية لبحوث الرأي العام | جامعة القاهرة،كلية الإعلام، مركز بحوث الراى العام | 1110-5844 | 2682-4655 | 2023 | 7 |
| 8 | الدراسات الإعلامية | مجلة البحوث الإعلامية | جامعة الأزهر | 1110-9297 | 2682-292X | 2023 | 7 |
| 9 | الدراسات الإعلامية | مجلة البحوث و الدراسات الإعلامية | المعهد الدولي العالي للإعلام بالشروق | 2357-0407 | 2735-4016 | 2023 | 7 |
| 10 | الدراسات الإعلامية | مجلة إتحاد الجامعات العربية لبحوث الإعلام و تكنولوجيا الإتصال | جامعة القاهرة، جمعية كليات الاعلام العربية | 2356-9891 | 2682-4639 | 2023 | 7 |
| 11 | الدراسات الإعلامية | مجلة بحوث العلاقات العامة الشرق الأوسط | Egyptian Public Relations Association | 2314-8721 | 2314-873X | 2023 | 7 |
| 12 | الدراسات الإعلامية | المجلة المصرية لبحوث الاتصال الجماهيري | جامعة بني سويف، كلية الإعلام | 2735-3796 | 2735-377X | 2023 | 7 |
| 13 | الدراسات الإعلامية | المجلة الدولية لبحوث الإعلام والاتصالات | جمعية تكنولوجيا البحث العلمي والفنون | 2812-4812 | 2812-4820 | 2023 | 7 |

# إدارة البصمة الرقمية لمستخدمي الإنترنت في ضوء نظرية إدارة خصوصية الاتصالات - دراسة ميدانية على عينة من مستخدمي الإنترنت بجمهورية مصر العربية

# Digital Footprint Managing of Internet Users in Light of the Theory of Communication Privacy Management

## A Field Study on a Sample of Internet Users in the Arab Republic of Egypt


د/ وسام محمد أحمد حسن

مدرس الصحافة في كلية الإعلام - جامعة الأهرام الكندية

Email: wesam@acu.edu.eg

**ملخص الدراسة**

يستكشف هذا البحث الدور المحوري للتكنولوجيا في مختلف جوانب حياة الناس، ويسلط الضوء على هيمنة الميزات التكنولوجية، حيث تتم الاتصالات وتنتشر المعرفة وتصاغ الأفكار على نحو اعتيادي في بيئة رقمية، وتؤدي شركات التكنولوجيا والاتصالات الكبرى دورًا حاسمًا في هذا المشهد. ومن خلال الاعتماد على آليات خوارزمية لتتبع تصرفات المستخدم وسلوكياته، فضلًا عن تسجيل البيانات ودمج آثار وجودهم على الإنترنت وعمليات تفاعل الأفراد في البيئة الرقمية في ملف شخصي متكامل، وفي ظل صعوبة إسناد حماية البيانات للقوانين والتشريعات وحدها في هذا الفضاء الافتراضي؛ هدفت هذه الدراسة إلى فهم كيفية إدراك المستخدمين لبصمتهم الرقمية، والأنشطة الرقمية التي تعمل على تشكيلها، فضلاً عن تصوراتهم للتأثيرات المحتملة ومستوى إدارتهم لبصمتهم الرقمية.

وقد أشارت النتائج إلى اعتبار وعي الأفراد أداة داعمة للتحكم في آثاره الرقمية، لا سيما مع وجود عديد من المعلومات يمكن أن تكون حساسة بالنسبة للمستخدمين، مثل المعلومات المالية والحسابات المصرفية، والصور والفيديوهات الشخصية. ولأن المعلومات الشخصية لا تحمل الدرجة نفسها من الأهمية، فإن بعض المعلومات يمكن الكشف عنها أو حجبها وفقًا للمخاطر التي يتصورها المستخدم إزاء الإفصاح عنها أو قناعته بوجود فائدة ستعود عليه، لذا تظهر أهمية وزن القرارات وتطوير المستخدمين لقواعد إدارة بصمتهم الرقمية بما يتناسب مع احتياجاتهم.

الكلمات المفتاحية: البصمة الرقمية، نظرية إدارة خصوصية الاتصالات، المراقبة الرقمية، الآثار الرقمية، تسييل البيانات، الحقوق الرقمية، الخصوصية الرقمية.

**Abstract**

This research explores the pivotal role of technology in various aspects of people's lives, highlighting the dominance of technological features in the present century. It emphasizes the nature of communication, knowledge sharing, and idea generation within a digital environment. Major technology and communication companies play a crucial role in this landscape by relying on algorithmic mechanisms to track user actions and behaviors, as well as to record data.

Due to the exchange of data among various entities involved in building user profiles and the challenges in assigning data protection solely to laws and regulations in the virtual space, the study aims to understand how users understand and manage their digital footprint, as well as their perception of potential impacts and their level of management of their digital footprints in this digital environment.

The findings presented evidence to support the consideration of individuals' awareness as a supportive tool for controlling their digital impacts, especially given the sensitivity of various information for users, such as financial information, personal images, and videos.

Since not all personal information carries the same level of importance, some information can be disclosed or concealed based on the anticipated consequences of such disclosure and data availability. Therefore, the importance of decision-making and individuals developing privacy norms that align with their needs becomes apparent.
Key Words: Digital footprint, Surveillance Capitalism, data monetization, Digital Trial, Digital Breadcrumbs, communication privacy management, digital rights, Digital Privacy

## مقدمة:

وفقًا لبيانات موقع Statista للربع الثاني من عام ٢٠٢٣، وصل عدد مستخدمي شبكة الإنترنت ٥.١٨ بليون مستخدم حول العالم، ونتيجة لتنامي استخدامات الإنترنت المختلفة، كتصفح الويب والاستعانة بمحركات البحث والاعتماد على البريد الإلكتروني، إضافة إلى الدور المهم الذي باتت تؤديه شبكات التواصل الاجتماعي في تمكين الفرد لإنتاج المعلومات ومشاركتها؛ إذ يشارك الأشخاص كل ما يمكنهم مشاركته على الإنترنت، مثل ما يشعرون به، وما يفعلونه، وهواياتهم وآراءهم، وما إلى ذلك؛ ما نتج عنه مليارات ومليارات من البيانات يتم إنشاؤها يوميًا؛ فأصبح النظام الرقمي يولي أهمية غير مسبوقة للآثار الافتراضية الرقمية التي يتركها الأفراد، وباتت نقرات المستخدمين منتجًا ذا قيمة كبيرة، وأصبحت بياناتهم بمثابة عملة رقمية شخصية يدفعها المستخدم. فبات نشاط الفرد يُسجَّل وتُحفظ بياناته بانتظام، مثل موقع وجوده في الوقت الحالي، والجهاز الذي يستخدمه، والصفحات التي يصل إليها، والمدة التي يقضيها على هذه الصفحات، ومن هم أصدقاؤه، وما الذي يعجبه، وما الذي يبحث عنه، والصور والفيديوهات الذي يُحمِّلها أو يُنزِّلها، واهتماماته، وكيف يشعر، وما انطباعاته، ويبدو أن آليات جمع البيانات لا مفر منها طالما أن التطبيقات والمنصات الحالية تعد مكونات أساسية لعديد من الإجراءات اليومية، لذا تعكس البيانات التي تمثل سجل نشاط الفرد عبر الإنترنت بصمته الرقمية.

وقد وصفت "شوشانا زوبوف" كيف تستخدم شركات التكنولوجيا الضخمة معلوماتنا وتُحوِّلها إلى سلعة من البيانات للتنبؤ بسلوكنا والتأثير فيه، وصاغت مصطلحًا أسمته "رأسمالية المراقبة Surveillance Capitalism" (بمعنى احتكار القلة

للتجريد الرقمي لبياناتنا ومعالجتها والتنبؤ اعتماداً عليها)، وأشارت إلى أن عمالقة رأسمالية المراقبة هم: جوجل، وأبل، وفيسبوك/ ميتا، وأمازون، وميكروسوفت؛ التي يُشكِّل كل منها الآن أنظمة اقتصادية تمارس سيطرة احتكارية على أغلب مساحات وأنظمة عمليات المعلومات والاتصالات الرقمية(1).

ويعد تسييل البيانات جوهر نماذج أعمال الرأسمالية الرقمية، فكل ما يفعله المستخدمون الرقميون في الفضاء الإلكتروني يترك آثاراً من البيانات تُجمَع وتُحلل من خلال خوارزميات بهدف جمع بيانات المستخدمين بوصفها المادة الخام اللازمة للتقدم وتطوير التقنيات الرقمية(2). فلدى مواقع الويب ومحركات البحث والتطبيقات والأجهزة المعتمدة على الإنترنت ووسائل التواصل الاجتماعي سجل حافل من البصمات الرقمية للمستخدم؛ ومع ما تقدمه من خدمات ومحتوى متنوع لمستخدميها، يبقى نموذج الأعمال السائد لكسب المال هو نموذج أعمال البيانات وتحليل بيانات المستخدمين؛ الذي تعرض لانتقادات شديدة لما يثيره من تساؤلات أخلاقية في مجال الخصوصية والاختراق، وطريقة تصميمه للمنصات، بما يدفع المستخدم نحو قضاء مزيد من الوقت في استهلاكها وإدمانها، مما يؤدي إلى اتساع البصمة الرقمية(3).

وكانت اللجنة الوزارية لمجلس أوروبا قد أشارت في "**دليل حقوق الإنسان لمستخدمي الإنترنت**" إلى الحق في حماية البيانات واحترام سرية المراسلات والاتصالات؛ إذ تُعالَج البيانات بانتظام عند استخدام خدمات مثل: المتصفحات، والبريد الإلكتروني، والشبكات الاجتماعية، ومحركات البحث، وخدمات تخزين البيانات السحابية، والرسائل الفورية، وبروتوكولات الإنترنت الصوتية؛ وأشارت إلى أنه لا ينبغي معالجة البيانات إلا إذا نصَّ القانون على ذلك أو عند موافقة المستخدم، ويجب أن يكون المستخدم على علم بالبيانات التي تُعالَج أو تُنقَل إلى أطراف ثالثة، ومتى ومن يقوم بذلك ولأي غرض، وأن يكون قادراً على التحكم في بياناته (التحقق من دقتها، أو طلب التصحيح أو الحذف، أو عدم احتفاظ الجهات بالبيانات لمدة لا تزيد عن اللازم)(4).

ووفقًا لذلك، يمكن القول إنه على الرغم من هذه التدابير فإنها لا تضمن وكالة شاملة لمستخدمي الإنترنت على بياناتهم، فمع ما تقدمه بعض شركات التكنولوجيا

والاتصالات على سبيل المثال من إيضاح سياسات الاستخدام والإفصاح عن البيانات التي تجمعها؛ إلا أن تشابكها وتعددها، وربما تخصصها، قد يُشكِّل عائقًا أمام فهمها، وهو ما قد يجعل المستخدم عازفًا عن قراءتها ومنصاعًا نحو إعطاء الموافقة العمياء والقبول لهذه البنود، فأصبح منح الموافقة عملية ميكانيكية لا تعكس سيطرة حقيقية على جمع البيانات، كما أن مشاركة الأفراد بياناتهم بشكل طوعي يُعد أيضًا مثالًا على بيانات قد تستخدم لأغراض التتبع والمراقبة الرقمية.

**المشكلة البحثية:**

غمرت الابتكارات التكنولوجية السوق الاستهلاكية، فانتشرت الأجهزة الذكية والأجهزة القابلة للارتداء وإنترنت الأشياء من أجل تحسين نوعية الحياة ورفاهية الفرد، وكان نتيجة لمساعي شركات التكنولوجيا العالمية إنشاء بيئات غامرة عبر الإنترنت بهدف إقناع المستخدمين بقضاء أكبر قدر ممكن من الوقت في استخدام تطبيقاته المختلفة، مما دفع بالمستخدمين إلى مزيد من الانغماس في التواصل والرفاهية والتمرير لمحتوى غير متناه، والتفاعل معه، ومشاركة بياناتهم، ما نتج عنه تشكيل سجل لنشاط الفرد عبر الإنترنت، وهو ما يُعرف بالبصمة الرقمية.

وتُعرِّف الدراسة البصمة الرقمية بأنها الآثار الرقمية أو البيانات التي يتركها المستخدمون خلفهم نتيجة استخداماتهم المختلفة للإنترنت (مواقع الويب، والتطبيقات، ومواقع التواصل الاجتماعي، ومحركات البحث، وتطبيقات المراسلة، والألعاب الإلكترونية... إلخ) عبر الأجهزة المختلفة، وهذه البيانات قد تُرسل عمدًا (أي بصمة صريحة)، وتسمى البصمة النشطة أو البصمة الإيجابية وهي الإنتاج النشط لما أنشأه المستخدم وقدمه بنفسه، مثل: تحديثات الحالة، ومشاركة الفيديو والصور في الشبكات الاجتماعية، أو إرسال بريد إلكتروني، أو أنشطة التعليق بصفحة ويب، وغير ذلك من معلومات يفصح عنها المستخدم بنفسه، بحيث يمكن لمستخدمي الإنترنت الآخرين رؤيتها والتعرف عليها. وقد تكون غير عمدية (أي ضمنية) وتسمى البصمة السلبية أو البصمة غير النشطة، وهي البيانات التي يتركها خلفه دون قصد، مثل: بيانات موقعه الجغرافي عبر عنوان بروتوكول الإنترنت IP، ونوع المتصفح الذي يستخدمه، ومصطلحات وسجلات

البحث، وتاريخ زيارته للمواقع، ومدة بقائه فيها... إلخ؛ وتعد هذه البيانات غير مرئية لمستخدمي الإنترنت الآخرين؛ إلا أنها تعد بيانات مرصودة من قبل مشغلي هذه المنصات الرقمية ومزودي خدمات الإنترنت. إضافة إلى المعلومات التي يشاركها أفراد آخرون عن المستخدم، التي تسمى الظلال الرقمية. ومن خلال هذه البيانات الصريحة والضمنية يتم تكوين بيانات استدلالية ضخمة، وإنتاج معلومات إضافية مستقلة، وإنشاء ملفات تعريف خاصة بالأفراد يمكن أن تستخدم في فهم اتجاهاتهم والتنبؤ بها وتوجيهها.

وتعد الجهات الفاعلة الرئيسية في عملية تتبع المستخدم هي التي تستطيع الوصول إلى البصمات غير النشطة التي لم يشاركها المستخدم بنفسه، وربما تمثل الغاية من تحليل بيانات المستخدمين إدامة تعزيز قوة غرف رجع الصدى، وتخصيص المحتوى بما يتوافق مع اتجاهات المستخدم واحتياجاته ويناسب رغباته، أو العمل على تحسين تجربة المستخدم عبر تحسين جودة الخدمات المقدمة له وتطوير أخرى جديدة؛ وهو ما يمكن أن يثير تساؤلات حول ملكية الفرد لبياناته ومستوى تحكمه فيها.

**وتأسيسا على ذلك، تتحدد المشكلة البحثية في معرفة كيفية إدارة المستخدمين لبصمتهم الرقمية، وذلك عبر استقصاء مستوى معرفتهم بالبصمة الرقمية والأنشطة الرقمية التى تعمل على تشكيلها، ومدى حساسية بعض البيانات لهم، إضافة إلى رؤيتهم لتأثيراتها المحتملة، ومستوى إدارتهم لها.**

**أهمية الدراسة:**

أولًا: تستمد الدراسة أهميتها من توالي المستحدثات الاتصالية وتطبيقاتها، وعدّها بنية أساسية للمجتمع المعاصر تدلل على تطوره وازدهاره، فقد بات الاعتماد على أنشطة الإنترنت في الحياة اليومية عادة لا يمكن تجنبها والعيش دونها، وربما يزداد هذا الشعور حين نفقد هذه القدرة على التواصل نتيجة خلل قد يصيب الإنترنت أو أحد التطبيقات التي نستديم في استخدامها، لتترك تساؤلًا مفاده: "كيف كنا نُسيّر حياتنا قبلها؟"؛ ومع السعي الجاهد من شركات التكنولوجيا للسيطرة على بيانات المواطنين الرقميين بوصفها مادة خام لرأسمالية منصاتهم، لذا كان من المهم إلقاء الضوء على مستوى إدراك المستخدمين للآثار الرقمية التي يخلفونها وراءهم ومدى حساسيتها، لا سيما في ظل صعوبة محو هذه الآثار.

ثانيًا: تستمد الدراسة أهميتها أيضًا من ضرورة فهم كفاية المنفعة التي يتيحها الجانب الإيجابي لهذه الآثار الرقمية، مقابل المخاطر التي قد تثير مخاوف المستخدمين من تشكيلها واتساعها، وهو ما يمكن أن يؤثر في قرارات المستخدم وإدارته لها وفقًا لسياقات مختلفة.

ثالثًا: كما تعزي الباحثة الأهمية العلمية للدراسة في طرق موضوع يتسم بالمحدودية البحثية، وهو البصمة الرقمية، باعتبار وجودها وتشكلها أمرًا حتميًا؛ مما يمكن أن يمثل إثراء للمجال البحثي المختص بتأثيرات تكنولوجيا الاتصالات وملكية البيانات والخصوصية؛ لا سيما وقد انتهى علم الباحثة إلى أن الدراسات في مجال البحوث الإعلامية العربية تتناول إطار الخصوصية الرقمية وحماية البيانات الشخصية، خاصة عبر مواقع التواصل الاجتماعي، وهي بذلك تركز في معظمها على البصمة الرقمية النشطة التي يشكلها المستخدم بنفسه دون التطرق إلى البصمة الرقمية غير النشطة، التي يمكن تشكيلها عبر الأدوات والمنصات الرقمية المختلفة ليس فقط مواقع التواصل الاجتماعي، وتعد أهمية دراسة جميع هذه الأشكال تأسيسًا على استخدامات الجمهور المتعددة الذي من خلال تفاعلاته على منصة ما يمكن أن يلمس أثر ذلك في منصة أخرى، لذا تتشابك البصمة الرقمية بجميع أشكالها، مما استدعى الباحثة لدراسة جميع أشكال البصمة الرقمية التي تتكون نتيجة استخدامات الإنترنت كوسيلة اتصال شاملة.

رابعًا: إمكان بلورة مجموعة من المقترحات والتوصيات يمكن أن تستفيد منها الجهات التي تأخذ على عاتقها مهمة التربية الإعلامية لمساعدة الأشخاص على الإبحار عبر الإنترنت بأمان.

**أهداف الدراسة:**

**تسعى الدراسة لتحقيق هدف رئيسى يتمثل في رصد مستويات تحكم المستخدمين في بصماتهم الرقمية، وذلك من خلال تحقيق مجموعة من الأهداف الفرعية على النحو الآتى:**

- التعرف على الاستخدامات الرقمية للمبحوثين.
- معرفة مدى حساسية أنواع البيانات المختلفة لدى المستخدمين بصفتها البيانات المطلوب حمايتها.

- التعرف على اعتقاد المبحوثين عن المدة الزمنية التي يسمح فيها للجهات المختلفة حفظ وتسجيل بيانات المستخدمين.
- اكتشاف مستوى معرفة المبحوثين بالبصمة الرقمية.
- معرفة وعي الجمهور بالأنشطة التي يعتقد أنها تعمل على تشكيل بصمته الرقمية.
- التعرف على تأثيرات البصمة الرقمية، سواء الإيجابية التي يمكن أن تمثل فائدة نفعية للمبحوثين، أو التأثيرات السلبية التي يمكن أن تدلل على المخاطر المتوقعة.
- التعرف على أسلوب المبحوثين في اتخاذ القرار بالإفصاح عن معلوماتهم، سواء إذا كان قراراً عقلانيًا وفقًا لقواعد، أو قراراً حدسيًا بديهيًا لا يعني المستخدم، ما قد ينتج عن تسجيل أنشطته الرقمية.
- معرفة مستوى إدارة المستخدم لبصمته الرقمية عبر التعرف على آليات التحكم المختلفة التي يقوم بها أثناء استخدامه للإنترنت.

**الدراسات السابقة:**

تتناول الباحثة الدراسات السابقة في ثلاثة محاور رئيسية؛ فيتناول المحور الأول الدراسات التي تطرقت لقياس وعي الأفراد بالبصمة الرقمية وتأثير الرغبة في التتبع الرقمي من قبل شركات التكنولوجيا والاتصالات على اتساع البصمة الرقمية للأفراد وعدّها شكلًا من أشكال المراقبة الرقمية وتتبع البيانات، إضافة إلى الخصوصية الرقمية، بينما تتناول دراسات المحور الثاني مجالات الاعتماد على البصمة الرقمية كوسيلة لجمع البيانات وتحليلها، مثل البيانات الديموغرافية والكشف عن نشاط المستخدمين، فيما تُركِّز دراسات المحور الثالث على التشريعات المتعلقة بالخصوصية والحق في محو هذه الآثار الرقمية، فقد أثارت قضية الموت الرقمي والحق في النسيان حق الفرد في التحكم ببصمته الرقمية إذا رغب في حذف شيء منها.

**أولًا: الوعي بالبصمة الرقمية وعدّها وسيلة للمراقبة الرقمية والخصوصية الرقمية:**

هدفت بعض الدراسات إلى التعرف على مجموعات من المستخدمين بالبصمة الرقمية: فتناول بعضها البصمة الرقمية للأطفال من خلال جمهور الآباء والأمهات كونهم

أوصياء على الوجود الرقمي للأطفال، واستراتيجياتهم لحماية تفاعلات أبنائهم الرقمية وسمعتهم المستقبلية. فذهبت نتائج دراسة (Buchanan, R. et al. 2019)[5] إلى محدودية معرفة الآباء والمعلمين بالبصمة الرقمية. وركَّزت دراسة (Chalklen, C., & Anderson, H., 2017)[6] على استخدام الأمهات لفيسبوك وعلاقته بالآثار الرقمية لأطفالهم، وسلَّطت الضوء على المخاطر الناجمة عن مشاركة المعلومات التي قد تضر بسمعة أبنائهم على المدى الطويل وتأثيراتها السلبية في مستقبلهم، وبينما أشارت الأمهات إلى تخوفهن من تأثيرات البصمة الرقمية إلا أن الشعور بالمتعة والاستمتاع بالتعليقات التي يحصلن عليها من خلال نشر الصور والفيديوهات لأطفالهن يدفعهن إلى مشاركتها دون التفكير بتأثيراتها في أطفالهن في المستقبل. فيما أشارت دراسة (Buchanan, R. et al., 2017)[7] إلى ارتفاع معرفة الأطفال بآثارهم الرقمية، كما عرضت الدراسة أشكال المراقبة أو الإشراف التي يقوم بها الوالدان، التي كان من أبرزها استخدام الآباء برنامجًا لتتبع البريد الإلكتروني لأطفالهم واستخداماتهم للإنترنت، بينما اكتفى بعض الآباء بتوجيه أبنائهم حول كيفية التصرف في الفضاء الإلكتروني.

وقد أشارت بعض الدراسات إلى طبيعة المعلومات التي يمكن أن تمثل قلقًا للمستخدمين في البيئة الرقمية: فأجابت دراسة (Marinelli, A., & Parisi, S. 2022)[8] عن اتجاهات مستخدمي الإنترنت الإيطاليين نحو مطالبات التطبيقات مشاركة بياناتهم الشخصية، فعبَّروا عن قلقهم بشأن جمع التطبيقات والمنصات عبر الإنترنت للبيانات الشخصية واستخدامها؛ ورغم اعتقاد المستخدمين بأهمية البيانات المرتبطة مباشرة بهوية الأشخاص الحقيقية فإنهم يظهرون موقفًا من التنازل عنها اعتقادًا منهم أنه لا يوجد كثير مما يمكنهم فعله حيال ذلك، أو نتيجة لتركيزهم على المزايا، مثل الوصول السريع للمعلومات.

وأشارت دراسة لهيئة الاتصالات والإعلام الأسترالية (ACMA, 2013)[9] إلى أن أكثر المعلومات المثيرة للقلق بالنسبة للمستخدمين هي المرتبطة بالمكان الجغرافي التي تُخزَّن من خلال الهواتف الذكية؛ إذ يمكن ربطها بهوية الأفراد عبر الإنترنت وبيعها

لشركات مجهولة. بينما كان قلق المبحوثين وفقًا لدراسة ( Camacho, M., et al., 2012)[10] هو القلق تجاه التأثير الذي قد تتركه بصمتهم الرقمية تجاه حياتهم المهنية.

وتناولت بعض الدراسات استخدام بيانات البصمة الرقمية كشل من أشكال مراقبة الأفراد، والاستعانة بها في تعزيز أساليب بقائهم داخل الوسيلة، مما يعني إتاحة الفرصة لتجميع بياناتهم بصورة أكبر، وتعزيز نموذج الأعمال الذي تقوم عليه لأغراض غالبًا ما تكون تجارية؛ فتناولت دراسة (Holloway, D. 2019)[11] تتبع البصمة الرقمية للأطفال بوصفهم مصادر للبيانات في اقتصاد البيانات الضخمة؛ إذ نجم عن ظهور ألعاب الأشياء (IoToys) -الألعاب المادية الملموسة والمتصلة بالإنترنت- تضخيم مكانة الأطفال بشكل كبير كمصادر للبيانات، مما أدى إلى خلق عديد من الفرص لتتبع الأطفال عبر الآثار التي يتركونها نتيجة تواصلهم الاجتماعي عبر الإنترنت، واستخداماتهم لمنصات جديدة دون شاشات، مثل الأجهزة القابلة للارتداء، والمساعدين الافتراضيين، والألعاب المتصلة، ففي الوقت الذي تخلق فيه الصناعة فرصًا للمشاركة الثقافية للأطفال عبر الإنترنت، فإنها تجمع كميات هائلة من معلومات المستخدم/ الطفل، إما خلسة أو بموافقة الأطفال أو الآباء الذين يدركون أن اختيار عدم المشاركة في جمع البيانات ومشاركتها قد تقلل من تجربة المستخدم، إضافة إلى ذلك، أشارت الدراسة إلى وجود سوق سوداء رقمية آخذة في الظهور، فبيانات الأطفال تُداول داخل دوائر تداول خرق البيانات، أو يُحتفظ بها مقابل فدية بعملة البيتكوين.

وتناولت الورقة البحثية (Montag, C., & Elhai, J. D., 2023)[12] كيف يدفع تصميم وسائل التواصل الاجتماعي إطالة مدة الاستخدام، وهو ما يعني اتساع حجم البيانات التي تُجمَع حول سلوك المستخدمين، ومن بين عناصر التصميم التي أشارت إليها: زر الإعجاب، وعدد المتابعين، والألوان المستخدمة، والدفع بالقيود الزمنية للمحتوى لإثارة الخوف من ضياع فرصة مشاهدة المحتوى، وهو ما يجلب الأشخاص إلى المنصات. كما أشارت دراسة (Montag, C., et al. 2019)[13] إلى الاعتماد على البصمة الرقمية للأفراد من أجل تخصيص المحتوى والتقليل من المحتوى الذي لا يهتمون به دون حاجتهم للقيام بهذا الإجراء بأنفسهم، وهو ما يعزز بقاء المستخدم لفترة طويلة داخل

المنصة. وهو ما أشارت إليه دراسة سابقة لـ ( Michael, M., & Lupton, D. 2017)[14] ألقت الضوء على اعتقاد الأفراد أن شركات مثل جوجل وفيسبوك تتتبع تفضيلاتهم وعاداتهم والمحتوى الذي يحملونه، وتتجلى هذه المراقبة بوضوح من خلال الإعلانات الموجهة للأفراد عند استخدامهم لهذه المنصات، بينما ما لم يكن واضحًا لهم تعقيدات مشاركة البيانات وأي أطراف أخرى قد تصل إلى بياناتهم.

ونتيجة لهذه المراقبة والتتبع، أشارت دراسة (Di Bene, E. 2022)[15] إلى تأثير المراقبة الرقمية من قبل المواقع والمنصات المختلفة في سلوك المستخدم عبر الإنترنت، فكشفت أن المراقبة الرقمية وتجميع بياناتهم خلقت حالة من عدم الثقة بين مستخدمي الإنترنت والمنصات الرقمية المختلفة.

ولما كان من المعروف أن أغلب التطبيقات ومواقع الويب وشبكات التواصل الاجتماعي تُعَدّ خدمات مجانية لجمهور المستخدمين، لذا كان من الضروري على هذه الشركات البحث عن نموذج أعمال يكون بمثابة الاقتصاد العائد إليها، لذلك تعد البيانات الناتجة عن تتبع البصمة الرقمية بمثابة العائد الذي تجنيه هذه الشركات، وهو ما يعني انتهاكًا محتملًا للبيانات من هذه الشركات نفسها، أو شركات وقراصنة يستهدفون البيانات المُخزَّنة لدى هذه المواقع والتطبيقات، وفي هذا الإطار تشير الباحثة إلى دراسة (Sindermann, C., et al. 2020)[16] التي هدفت إلى معرفة مدى قناعة المستخدمين بسداد مقابل مادي لاستخدام وسائل التواصل الاجتماعي إذا كانت بياناتهم ستبقى خاصة وبأمان، إلا أن نسبة قليلة من المبحوثين (21.43%) أيدوا هذا النموذج ورفضت الأغلبية فكرة دفع مقابل مادي للاستخدام.

ومن هنا يمكن الحديث عن أهمية ما أكدته دراسة ( Andrew, J., et al. 2021)[17] من ضرورة إفصاح شركات التكنولوجيا عن أي حالة اختراق لبيانات المستخدمين، لأنه من الصعب على المستخدم تحديد إذا كانت البيانات التي قدمها للمؤسسة اختُرقت أم لا.

وتناولت مجموعة من الدراسات الإعلامية العربية الخصوصية الرقمية، لا سيما عبر مواقع التواصل الاجتماعي، ومنها دراسة (غادة النشار، ٢٠١٨)[18]، حول تقصي مفهوم الخصوصية لدى مستخدمي فيسبوك وحدود إفصاحهم عن المعلومات من خلاله، وذهبت النتائج إلى ارتفاع مستوى فهم إعدادات الأمان على موقع فيسبوك، وفهم مخاطر الإفصاح عبر فيسبوك، وأيضاً جريان العرف بين الأصدقاء على نشر المعلومات والأفكار والصور الخاصة أو نشر الأمور الشخصية.

وأشارت كل من دراسة (هاني إبراهيم ، ٢٠٢٢)[19] عن اتجاهات الشباب نحو انتهاك الحياة الخاصة عبر شبكات التواصل الاجتماعي، ودراسة (هدير أحمد، ٢٠٢٢)[20] عن إدارة المرأة المصرية لخصوصيتها على مواقع التواصل الاجتماعي فيسبوك، ودراسة (سالي سعد، ٢٠٢١)[21] حول انتهاك الخصوصية الرقمية عبر فيسبوك وسناب شات، ودراسة (سحر أحمد غريب، ٢٠٢١)[22] حول إدراك الجمهور لانتهاكات الخصوصية الرقمية عبر الإعلام الجديد، إلى إدراك مفهوم الخصوصية الرقمية وارتفاع وعي الجمهور بمخاطر انتهاكها عبر مواقع التواصل الاجتماعي والإعلام الجديد، وسيادة الاتجاه الإيجابي في التعامل مع إعدادات الأمان والاهتمام بضبط إعدادات الخصوصية عبر هذه المواقع.

وتناولت دراسة (سليمة حسن، ٢٠٢٢)[23] حدود تداول المعلومات الشخصية للمرأة الليبية على صفحات فيسبوك، من خلال دراسة تحليلية لبعض الصفحات الشخصية، وأشارت إلى شيوع استخدام الاسم الصريح، والصفة الاجتماعية والأكاديمية، ومكان الإقامة، والشأن، وأفراد الأسرة، والاهتمامات والهوايات والآراء؛ إلا أنه توجد محدودية كبيرة في عرض الصور الشخصية التي كانت نسبتها ٣% فقط من مجموع الصفحات الخاضعة للتحليل. وتمثل انتهاك الخصوصية في ما تقوم به بعض النساء من مشاركة بيانات أخريات وإن كان بغرض المدح، مثل التهنئة أو الإشادة، وسواء كان الهدف يترجم حسن النوايا أو لتحقيق أغراض أخرى، إلا أن هذا السلوك يندرج تحت اختراق الخصوصية. فيما أشارت (مها مصطفى وهناء عكاشة، ٢٠٢٢)[24]، في دراستهما عن

مخاطر انتهاك الخصوصية لمستخدمي التطبيقات الرقمية، إلى أن أهم المخاطر التي تعرض لها الشباب المصري كانت سرقة البيانات الشخصية، واستخدام خاصية (تصوير الشاشة "سكرين شوت") لقصة له أو لصورة ومشاركتها عبر صفحة أخرى دون إذنه، وكانت أهم الإجراءات التي اعتمد عليها مستخدمو التطبيقات الرقمية للحد من مخاطر انتهاك الخصوصية هي عدم فتح الرسائل مجهولة المصدر، وعدم الرد على الرسائل التي تحتاج إلى معلومات شخصية أو مهمة.

أما في سياق انتهاك الخصوصية المرتبط بالتسويق الإلكتروني، وتحليل البيانات الضخمة وتأثيره في الخصوصية، فقد أكدت نتائج دراسة (محمود محمد، ٢٠٢٢)[25] النتائج ذاتها المتعقلة بإدراك الجمهور لانتهاك الخصوصية عبر مواقع التواصل الاجتماعي، وأن لدى الشباب مستوى مرتفعاً من الوعي بالتهديدات التي تتعرض لها خصوصيتهم الرقمية، ورغم إدراكهم حساسية معلوماتهم الشخصية فإنهم يقدمونها طواعية لعديد من المواقع عبر شبكة الإنترنت. كما أشارت دراسة (مها عبد الحميد، ٢٠٢٢)[26] إلى إدخال المبحوثين بياناتهم الشخصية على التطبيقات التسويقية.

**ثانيا: دراسات تحليل البصمة كوسيلة لجمع المعلومات:**

تناولت دراسات هذا المحور تحليل البصمة الرقمية – لا سيما البصمة النشطة– فأشارت دراسة (Hinds, J. 2018)[27] إلى إمكانية التنبؤ بالسمات الديموغرافية للمستخدمين من خلال نشاطهم عبر الإنترنت، بالتطبيق على قواعد البيانات العلمية؛ إذ رصد الباحثان ١٤ سمة، منها: الجنس، والعمر، والموقع الجغرافي، والتوجه السياسي، والعِرق، والتعليم، والدخل، واللغة، والمهنة. وأجرى مركز بيو للأبحاث (PEW, 2017)[28] دراسة تحليلية لمعرفة تدفقات اللاجئين من الشرق الأوسط إلى أوروبا، من خلال تتبع عمليات البحث على الإنترنت التي أجريت باستخدام اللغة العربية في دول مثل ألمانيا أو تركيا، وأشارت إلى أن مصطلح البحث "الألمانية" هو على الأرجح كلمة يبحث عنها المهاجرون الجدد عندما يحاولون ترجمة نص من العربية إلى الألمانية عبر الإنترنت أو تعلم كلمات ألمانية جديدة. وحللت دراسة (Hilbert M. et al., 2017)[29] البصمة الرقمية للحركات الاجتماعية أثناء الاحتجاجات الشعبية في تشيلي عبر تويتر،

ورصدت أكثر من ١٥٠ ألف تغريدة تعبر عن تسع حركات اجتماعية في تشيلي. بينما حللت دراسة (Robards, B, et al. 2021)[30] صور السيلفي لمجموعة من المستخدمين كونها تمثيلات للذات رقمياً، وعدّها شكلًا من رواية القصص الرقمية يمكن من خلالها استكشاف بيانات حول الصحة العقلية والتجارب الشخصية ومشاعر المستخدم.

وتناولت دراسة (Wang X. et al., 2016)[31] الآثار الرقمية للمقالات العلمية على مواقع التواصل الاجتماعي، ومثلها سعت دراسة (Fang, Z. et al., 2016)[32] لتتبع البصمة الرقمية للمقالات الأكاديمية، واستعرضت دراسة (Lambiotte, R., & Kosinski, M. 2014)[33] العلاقة بين البصمة الرقمية والتنبؤ بشخصية المستخدمين، وأشارت إلى أن مجموعة واسعة من البصمات الرقمية المنتشرة والمتاحة للعامة في كثير من الأحيان، مثل الملفات الشخصية على فيسبوك، يمكن استخدامها لاستنتاج الشخصية وتقييم السمات النفسية بشكل تلقائي وسريع.

وربطت دراستان بين تتبع البصمة الرقمية للتعرف على النشاط السياحي للدول، فتناولت دراسة (Önder I. et al., 2016)[34] تتبع الصور على موقع فليكر Flickr بوصفها تمثل أحد أنواع البصمة الرقمية النشطة كمؤشر للنشاط السياحي بالنمسا من خلال تقدير أعداد السياح في الوجهة. وتناولت دراسة (F. Girardin et al., 2008)[35] الكشف عن النشاط السياحي من خلال البصمة الرقمية لبيانات الوجود المكاني والزماني التي ينشئها السياح بروما، فقد أمكن التعرف على عدد السائحين الذين زاروا منطقة جذب معينة وجنسياتهم، واستنتاج تجاربهم من خلال الصور التي تم تحميلها والأوصاف الدلالية لها.

وعلى العكس من ذلك، رأت دراسة (Golder, S., & Macy, M., 2014)[36] صعوبة الاعتماد على البيانات الخاصة بالبصمة الرقمية النشطة، مثل المعلومات الديموغرافية، لأن عديداً من المستخدمين قد يشاركون بمعلومات زائفة أو غير مكتملة أو غامضة، كما قد يصعب الفصل بين الحسابات الوهمية والحسابات الحقيقية، مما يجعل

من الصعب على الباحثين إيجاد الارتباط بين محتوى التغريدات والسمات الديموغرافية مثل العمر أو الجنس.

**ثالثًا: دراسات متعلقة بحماية الخصوصية في السياق الرقمى والحق في محو البصمة الرقمية:**

ناقشت دراسة (هبة جودة، ٢٠٢٢)(37)، حول الحماية القانونية للخصوصية الرقمية في الدول العربية، تشريعات الإنترنت الصادرة عن بعض الدول العربية ومنها مصر، وأشارت النتائج إلى اعتبار حماية الخصوصية الرقمية للمستخدمين جزءاً أصيلًا من حقوق الإنسان، والتعدي على الخصوصية الرقمية جريمة من ضمن جرائم تقنية المعلومات يخضع من يرتكبها للعقاب بموجب القانون، وقد رصدت الدراسة في تحليلها استحداث مصطلحات قانونية بقانون دولة الإمارات مثل "الروبوت الإلكتروني" و"الدليل الرقمي". وأشارت دراسة (غزيل عائشة، ٢٠٢٣)(38) إلى أهمية تناسب قوانين حماية الحق في الخصوصية الرقمية مع التطورات الرقمية للمجتمع الحالي، ومن ثمَّ فقد هدفت إلى تحليل مضمون الأطر الدولية التي تهدف إلى الاعتراف بالحق في الخصوصية، وقد أشارت إلى أن الحق في الخصوصية ليس حقًا مطلقًا، وإنما مقيد بمجموعة من القيود، منها ضرورة وجود علاقة عقلانية بين الوسائل المستخدمة والهدف المنشود، فنصت اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات -على سبيل المثال- على أن يكون جمع البيانات وفقًا لأهداف محددة وغير مفرطة، كما توصلت إلى نتائج عامة مفادها اعتراف قواعد القانون الدولي بالخصوصية حقًا من حقوق الإنسان، إلا أنها عاجزة عن مواكبة ما طرأ على هذا الحق من مستجدات في البيئة الرقمية. ورصدت دراسة (أسماء عشري، ٢٠٢٢)(39) اتجاهات النخب نحو تشريعات حماية البيانات عبر مواقع التواصل الاجتماعي، وذهبت إلى اعتقاد المستخدمين أن سياسة حماية الخصوصية عبر مواقع التواصل الاجتماعي يشوبها نوع من التضارب، فقد يتعارض نص قانوني مع نص آخر، وهو ما يجعلهم حذرين تجاه الإفصاح عن بياناتهم الشخصية.

وناقشت بعض الدراسات ضرورة تأصيل حق الأفراد في النسيان، بوصفها قيمة اجتماعية إزاء ما قدموه عن أنفسهم في صورة البصمة الرقمية النشطة، أو ما يقدمه الآخرون عنهم في صورة الظلال الرقمية؛ فأشارت دراسة (Stainforth, E. 2022)[40] إلى أن شركات مثل جوجل أوجدت ساحة جديدة للمنافسة الاقتصادية والسياسية على الإنترنت، ما نتج عنه المنافسة على ممارسات جمع البيانات الخاصة بالأفراد، لذلك أصبحت مسألة النسيان مهمة؛ والأساس المنطقي لحق النسيان هو الاعتراف بالحدود بين المعلومات الشخصية والعامة، لأن وجود مثل هذا الحق له أهمية كبيرة في محاولة ترسيم هذه الحدود المتغيرة. بينما تناولت إحدى الدراسات وعي الجمهور بمصير بصماتهم الرقمية بعد وفاتهم، فأشارت نتائج دراسة (Grimm, C., & Chiasson, S. 2014)[41] إلى انخفاض وعي الجمهور بمصير بصمتهم الرقمية بعد وفاتهم، واعتبروا الاستبانة بمثابة المُعرِّف الأول الذي لفت انتباههم لقضية الموت الرقمي، وأشاروا إلى رغبتهم في حذف بصمتهم الرقمية بعد وفاتهم وتفضيلهم لوجود منظمة غير ربحية تحذف الحسابات، أو أن تفوض هذه المهمة إلى أقرب الأقرباء أو الأصدقاء.

وقد تناولت مجموعة من الدراسات الشقّ القانوني للحق في النسيان؛ فقدمت دراسة (Bunn, A. 2019)[42] نظرة عامة عن الحق في النسيان، في اللائحة العامة لحماية البيانات، وكيف من المحتمل أن يؤثر ذلك في الأطفال، مع الإشارة إلى أنه لا يوجد حق مماثل في أستراليا، وأوصت الدراسة بإدخال هذا الحق، لأن الافتقار إلى السيطرة على المعلومات الشخصية يمكن أن يؤثر في نمو الطفل، واحترام الذات، والشعور بفقدان السيطرة على الحياة وفقدان الاستقلالية. كما استعرضت الدراسة انتقادات وُجهت للحق في النسيان، فأشارت إلى أن تطبيق هذا الحق في العالم الرقمي قد يُشكِّل عائقًا وتعارضًا أمام حرية التعبير والمصلحة العامة في الوصول إلى المعلومات. واستعرضت دراسة (Mitrou, L., & Karyda, M. 2012)[43] تشريعات حماية البيانات كاستجابة قانونية للتحدي التكنولوجي الذي أحدثته التحولات العميقة في طريقة معالجة البيانات الشخصية واستخدامها، والحق في ضمان عدم الاحتفاظ بالمعلومات الشخصية. وناقشت

دراسة ( Koops, B. J. 2011)[44] المفاهيم والتحديات الأساسية لـ "الحق في النسيان" فيما يتعلق بالمصير المعلوماتي للأفراد، سواء الحق في حذف البيانات أو الحق في عدم التتبع، وانتهت إلى أن هذا الحق ليس موجوداً في الوقت الحالي نظراً لعدم كفاية قانون حماية البيانات لمنح هذا الحق للأفراد.

**ما يمكن استخلاصه من الدراسات السابقة:**

1- من الناحية المعرفية؛ أكدت الدراسات أهمية الأنظمة والتقنيات والشبكات التي تخلق مجموعة متنوعة من عوالم التواصل الافتراضية؛ إلا أنها أهمية لا تخلو من تخوف بشأن ما تفرضه اقتصاديات هذه المواقع والشبكات من تتبع لبيانات المستخدمين سواء لأغراض تجارية أو لتحسين تجربة المستخدم. وقد بيَّنت الدراسات تباينا في مستوى دراية المستخدمين بالبيانات التي تُجمع أثناء نشاطهم عبر الإنترنت، وقد أفاد البُعد المعرفي للدراسات السابقة الباحثة في بلورة وتحديد المشكلة البحثية.

2- لم تعتمد بعض الدراسات على إطار نظري، فغلب الطابع الاستكشافي لقياس وجود الظاهرة في المجتمع، لاسيما الدراسات الأجنبية التي تناولت البصمة الرقمية، بينما اعتمدت الدراسات العربية المتعلقة بالخصوصية على نظريات مثل الاعتماد على وسائل الإعلام، والاستخدامات والإشباعات، ونموذج الخصوصية الإلكترونية، وتأثير الشخص الثالث، وقد استدعى ذلك الباحثة لإيجاد مدخل نظري ملائم يفيد في الظاهرة محل الدراسة وتفسير نتائجها.

3- اعتمدت أغلب الدراسات على منهج المسح، واستخدمت الاستقصاء أداة رئيسية في الوصول للنتائج، بينما اعتمدت بعض الدراسات على مجموعات النقاش المُركَّزة، لا سيما الدراسات التي أُجريت علي الأطفال، وقد اعتمد عدد قليل من الدراسات على التحليل الكيفي للبصمة الرقمية للدلالة على بعض المتغيرات، كالسمات الديموغرافية أو اتجاهات الجمهور.

4- استفادت الباحثة من الدراسات السابقة في تحديد أداة جمع البيانات وبناء صحيفة الاستقصاء، كما تستفيد منها في مقارنتها مع نتائج الدراسة الحالية.

5- في أعقاب النتائج والرؤى التي توصلت إليها الدراسات السابقة بات من الضروري تأكيد أهمية الدراسة، بوصف البصمة الرقمية بعداً توضح من خلاله سياقات وممارسات المستخدمين الرقمية، التي تُنشأ من خلالها هذه البيانات، ومن ثَمَّ جمعها ربما دون وعي منهم.

**الإطار النظري للدراسة: نظرية إدارة خصوصية الاتصالات Communication Privacy Management Theory:**

تعد البصمة الرقمية مصدر قلق كبير لقدرتها على تسجيل نشاط الفرد وتشكيل ملفات تعريف شخصية للمستخدمين لتحليل اتجاهاتهم والتنبؤ بها وتوجيهها. ويعد التحكم في البيانات التي يرسلها المستخدم عبر الإنترنت مرهوناً بصورة معقولة بإدراكه للآثار التي يتركها خلفه، لا سيما المرتبطة بالبصمة الرقمية النشطة، فقليل من المستخدمين يدركون درجة اتساع نطاق آثارهم الرقمية ومشاركة بياناتهم لدى أطراف ثالثة وفقًا لما أشارت إليه الدراسات السابقة، ثم العمل على إيجاد الحلول للتحكم ببصمتهم الرقمية.

لذلك ترتكز الدراسة الحالية على نظرية إدارة خصوصية الاتصالات، التي صاغتها "ساندرا بترونيو" Sandra Petronio، وتقوم على اتباع نهج قائم على إدارة قواعد للكشف عن المعلومات التي تخص الفرد والتحكم فيها، وقد أشارت "بترونيو" إلى أن التحدث عن مشاعرنا الخاصة للعامة ليس بالأمر السهل، فغالبًا ما يكون الأمر محفوفًا بالمخاطر، فقد نشعر بالحرج أو عدم الارتياح كوننا مكشوفين بطريقة أو بأخرى؛ ويعد الاختيار بين الإخبار أو عدم الإخبار حالة كثيراً ما نواجهها. وتثير "بترونيو" تساؤلًا حول متى نسمح للآخرين بمعرفة الجانب الخاص لنا ومتى نبقه سراً؟ وهو ما يعني أن الكشف عن المعلومات ليس قراراً مباشراً، لكنه حالة من التوازن التي تجعل الفرد يسعى للموازنة بين متطلبات الموقف واحتياجاته واحتياجات الآخرين من حوله ليتخذ قرار الإفصاح من عدمه، وينبع ذلك كله من إحساس الفرد بأنه المالك الشرعي للمعلومات الخاصة به، ويمكن أن تشمل مخاطر الإفصاح: الكشف عن المعلومات الخاصة لشخص خطأ، أو الكشف في وقت غير مناسب، أو إخبار الكثير عن أنفسنا، أو تعريض الآخرين للخطر، لذا تفترض نظرية إدارة خصوصية الاتصالات أن الأشخاص يتخذون خيارات بشأن

الكشف أو الإخفاء بناء على المعايير والشروط التي يرونها[45]. ويعني ذلك أن لدى الأشخاص حاجتين متزامنتين، لكنهما متعارضتان وتؤثران في قرارات الكشف عن المعلومات وإخفائها، فالأشخاص يرغبون الإفصاح عن المعلومات بوصفها طريقة لتحقيق هدف ما، وفي الوقت ذاته يرغبون أيضًا في الاحتفاظ بشعور الخصوصية الذي يساعد على الاستقلالية الفردية، فتصف النظرية الطريقة التي يتعامل بها الأشخاص مع هذا التوتر[46].

واقترحت مؤسسة النظرية خمسة أسس يقوم عليها نظام إدارة القواعد أو الحسابات العقلية التي يجريها الفرد ليقرر ما إذا كان سيخبر بالمعلومات أو يحتفظ بها، وذلك على النحو: **أولًا: ملكية الخصوصية:** فالأفراد يعتقدون ملكيتهم للمعلومات، الذي يُعدّ استحقاقًا يحددون من خلاله ما يعرفه الآخرون عنهم (أي أن الفرد هو وحده المالك الحقيقي للمعلومات). **ثانيا: الحدود بين المعلومات الخاصة والعامة:** بمعنى إقامة حدود ينظمها الأفراد كي يتمكنوا من التحكم في قدر المعلومات التي يُفصح عنها، سواء عن أنفسهم أو عن الآخرين، وتفترض أنه عندما يصبح الأفراد أكثر تقدمًا في العمر غالبًا ما تتقلص الخصوصية بسبب الاحتياجات، مثل "الاحتياج للسلامة" كأن يطلب شخص كبير السن من شخص ما أن يهتم بشؤونه المالية، أو الاهتمام بمخاوفه الصحية... إلخ. **ثالثًا: الملكية والتحكم:** نظرًا لاعتقاد الأفراد أن المعلومات الخاصة مملوكة لهم، وقد يؤدي الكشف عنها إلى الشعور بالضعف، لذلك فإن السيطرة على الحدود والتحكم في تدفق المعلومات مهم لدرء احتمالات الضعف، وينبغي الإشارة أيضًا إلى حدود الخصوصية الجماعية، فإذا كانت لدينا ملكية شخصية للمعلومات التي تتعلق بالذات ونتوقع الحق في السيطرة عليها، فنحن في الوقت نفسه نتشارك في ملكية المعلومات التي تمت مشاركتها معنا (مثل خصوصية معلومات عن العائلة أو العمل أو مجموعة ما يكون الفرد عضوًا فيها... إلخ)، هذه المعلومات يُعدّ الفرد مالكًا مشاركًا فيها، ومن ثمَّ يكون التحكم فيها بشكل جماعي متبادل من قبل أولئك المطلعين عليها وأولئك الذين يعتبرون ضمن الحدود، فعندما يخبرنا آخرون بمعلومات خاصة فإننا نبرم عقد مسؤولية ضمنية بصفتنا مالكين مشاركين لهذه المعلومات، ويكون لدينا إمكانية اتخاذ قرارات، سواء بشكل مستقل عن

المالك الأصلي أو بالتعاون معه فيما يتعلق بالنشر لطرف ثالث، ويفترض أن المعلومات محمية وفقًا لرغبات المالك الأصلي(47)، فعلى سبيل المثال، عندما يتعامل الأفراد مع وسائل التواصل الاجتماعي فهم يتخذون قرارات بشأن سيطرتهم على خصوصيتهم ومن يمكنهم السماح له بالوصول إلى شبكة أصدقائهم أو متابعيهم، كونهم مالكين مشاركين محتملين لمعلوماتهم الخاصة، وقد يعني هذا استخدام الأدوات الموجودة في وسائل التواصل الاجتماعي لإخفاء معلومات معينة، وتعيين الحساب إلى عام أو خاص، وتحديد قواعد لتحديد المحتوى المناسب للنشر(48). **رابعا: قواعد التحكم في المعلومات الخاصة:** يؤكد هذا المبدأ أن الأفراد يعتمدون على نظام قائم على القواعد للتحكم في تدفق المعلومات الخاصة، بتحديد متى وكيف ومع من وبأي طريقة يمكن منح الآخرين أو منعهم من الوصول إلى المعلومات الخاصة لشخص ما، ويمكن أن تؤثر معايير مثل النوع الاجتماعي، والقيم الثقافية، وحسابات المخاطر مقابل المنافع، في أسس الأحكام المتعلقة بوضع القواعد وتنفيذها وتعديلها. وتؤدي عمليات الكشف عن المعلومات إلى الحاجة لتنسيق الحدود نظرًا لوجود وصاية متوقعة على المعلومات يفترضها كل من المُفصح والمتلقي، وفي هذا الإطار صاغت "ساندرا بترونيو" مصطلح اضطراب الحدود (بمعنى اضطراب الخصوصية)، بالافتراض أن هذا التنسيق لا يعمل دائمًا بطريقة متزامنة، وقد لا يتمكن الأشخاص في بعض الأحيان من تنسيق حدود الخصوصية معًا(49)، ويمكن أن يكون اضطراب الخصوصية نتيجة لأحداث أو سيناريوهات تجبر الفرد على إعادة التفكير وتعديل توقعاته وسياسات الخصوصية الخاصة به. على سبيل المثال، يمكن أن يكون ذلك نتيجة اختراق حسابه أو مشكلة في حياته الواقعية ناتجة عن شيء نُشِر على وسائل التواصل الاجتماعي(50). **خامسا: الخصوصية والإفصاح:** فبمجرد أن يكشف الشخص عن معلومات خاصة تصبح أقل خصوصية وأكثر عمومية، وتعتمد درجة العلنية على عدد من القضايا، مثل عدد الأشخاص المُطَّلعين على المعلومات، ومقدار المعلومات التي تم الكشف عنها، ومن يتلقى المعلومات ويجمعها(51).

وقد أعادت "بترونيو" صياغة النظرية في ثلاثة عناصر رئيسية تمثل معًا نظامًا لإدارة خصوصية الاتصالات، هي: (**أ- تنظيم حدود المعلومات الخاصة، ب- التحكم**، بوصفه المحرك الذي ينظم شروط منح أو رفض الوصول للمعلومات الخاصة، **ج- اضطراب الخصوصية**، بمعنى انهيار تنظيم الخصوصية)، وذلك على النحو الآتي(52):

1) يعتقد الأشخاص أنهم المالكون الوحيدون لمعلوماتهم، ويثقون في أن لديهم الحق في حمايتها أو منح حق الوصول إليها.
2) عندما يمنح "المالكون الأصليون" آخرين إمكانية الوصول للمعلومات، فإنهم يصبحون "مالكين مشاركين مفوضين"، ويفترض "المالك الأصلي" أن الآخرين لديهم مسؤوليات ائتمانية عن المعلومات.
3) لما كان الأفراد يعتقدون أنهم يمتلكون الحق في معلوماتهم، ويشعرون بشكل مبرر أنه يجب أن يكونوا هم من يتحكمون فيها؛ يظل هذا الافتراض قائمًا حتى بعد منح حق الوصول لمعلوماتهم للآخرين المُصرَّح لهم.
4) تعد الطريقة التي يتحكم بها الأشخاص في تدفق المعلومات الخاصة قائمة على تطوير واستخدام قواعد الخصوصية؛ وتُستمد هذه القواعد من معايير مثل الدوافع والقيم الثقافية والاحتياجات الظرفية.
5) ضرورة التنسيق والتفاوض بشأن قواعد الخصوصية مع "المالكين المشاركين"، فيما يتعلق بوصول طرف ثالث للمعلومات.
6) تؤدي الملكية المشتركة إلى حدود خصوصية جماعية تُدار بشكل مشترك.
7) تُنظَّم حدود الخصوصية الجماعية من خلال القرارات المتعلقة بمن قد يصبح مطلعًا على المعلومات، ومقدار المعرفة التي قد يعرفها الآخرون داخل وخارج الحدود الجماعية، وحقوق الكشف عن المعلومات.
8) قد تُنتهك التوقعات، وهو ما يشير إلى اضطراب الخصوصية.

ووفقًا لذلك، يمكن القول أنه عندما تكون معلومات الفرد متاحة في قاعدة بيانات إلكترونية، فإنهم يخشون فقدان السيطرة على كيفية استخدام تلك المعلومات في المستقبل، وبذلك يواجه المستخدمون مهمة مُعقَّدة تتمثل في التوفيق بين احتياجاتهم

المتعددة، لأن عملية الكشف عن البيانات تنطوي دائماً على درجة كامنة من المخاطر، تدفع الأفراد نحو العمل على تحديد الحدود التي تحكم معلوماتهم بشكل استباقي، وتنظيم إمكانية الوصول إليها، وتحفز وضع توقعات وبناء افتراضات متعلقة بالملكية المشتركة للمعلومات عند مشاركتها مع آخرين(53).

**نظرية إدارة خصوصية الاتصالات في الدراسة الحالية:**

كان نتيجة لنماء بيئة الإنترنت وتطبيقاتها المختلفة والتقنيات الحديثة المرتبطة بها، تزايد كمية البيانات الخاصة بالأفراد واتساع حدود تدفقها لجهات خارج حدود المستخدم، وعلى الرغم من كوننا نعيش في عالم من الإفصاحات الصاخبة والآثار الرقمية التي لا مناص من تركها؛ فإن الاعتقاد بملكية البيانات والحق في التحكم فيها، والاحتفاظ ببعض الحقائق، ووضع حدود مجازية تؤطر متى وكيف ومع من وبأي طريقة يمكن منح أو منع الآخرين من الوصول للبيانات، فيجب على مستخدمي الإنترنت التفاوض بشأن حدود الخصوصية الخاصة بهم عبر الإنترنت، من خلال استخدام قواعد واستراتيجيات مختلفة تحد من ممارسة الجهات المختلفة سيطرة على بياناتهم، لذا تستكشف الدراسة معرفة المستخدم بالبصمة الرقمية، والتعرف على قدرته في تحديد الأنشطة التي يقوم بها وتعمل على تشكيل بصمته الرقمية، وإدراكه لمن يمكنه تتبع البصمة الرقمية، وذلك من خلال **مقياس (الوعى بالبصمة الرقمية)**، ويُقصد به مقدار المعلومات التي يملكها الفرد حول البصمة الرقمية، واعتمدت الباحثة في صياغة هذا المقياس على مقياس دراسة (Surmelioglu, Y., and Suleyman S. 2019)، **ومقياس (الأنشطة التى تعمل على تشكيل البصمة الرقمية)**، إضافة إلى قياس الاستخدامات الرقمية للمبحوثين لفهم مستوى استخدام الأفراد للإنترنت والتكنولوجيا الرقمية.

ولما كانت النظرية تصف عملية اتخاذ القرار التي تقود الأشخاص للكشف عن أو إخفاء المعلومات التي يعدونها خاصة، عبر وضع هذه الحدود وتنظيمها على قدر الفوائد والمخاطر المتوقعة التي ستعود على المستخدم. ويفترض أن تكون مشاركة المعلومات فقط مع الأشخاص الذين يُنظر إليهم على أنهم أقرب للفرد، مثل الأصدقاء، ومقدمي الخدمات،... إلخ، وفي إطار القيود الضمنية لعدم إفصاح الآخرين عن معلومات خاصة

بهم، أو استخدامها بطريقة أخرى، تسعى الدراسة لاستكشاف كيف يزن الأفراد قراراتهم قبل الإفصاح عن البيانات، إذ يُمكن أن يكون قراراً عقلانياً قائماً على مجموعة من الأسباب المنطقية، كما يمكن أن يكون قراراً بديهياً لمجرد استمرار استخدام الخدمات الرقمية، وذلك من خلال صياغة **مقياس (أسلوب اتخاذ القرار)**.

كما يمكن وزن القرار وفقًا لمجموعة من العوامل، مثل معدلات المخاطر مقابل الفائدة، لذا تقوم الدراسة بتقييم المستخدم للتأثيرات المحتملة للبصمة الرقمية، والمفاضلة بين الفوائد المتصورة كتأثير إيجابي للبصمة الرقمية (تشير الفائدة المتصورة إلى الفوائد النفعية الشخصية التي يعتقد المستخدم من خلالها أهمية ترك آثاره الرقمية ليحصل في إثرها على مزايا إيجابية)، وتقييم المخاطر المتوقعة (أي اعتبار المخاطر المتوقعة أحد الأسباب التي يمكن أن تعزز إفصاح المستخدم عن معلومات أو استخدامه لأدوات رقمية من شأنها جمع بياناته)، وذلك من خلال صياغة **مقياس (تأثيرات البصمة الرقمية)**.

ويُقصد بالمعلومات التي يمكن أن تُشكِّل البصمة الرقمية للمستخدمين عند استخدامهم الإنترنت؛ إما تلك التي يكون المستخدم على علم بماهيتها نتيجة إفصاحه عنها فتشكل بيانات البصمة الرقمية النشطة، أو البيانات الناتجة عن سلوكه الإلكتروني، التي لا تعد طوعية الإفصاح، وتتكون عبر تتبع أنشطة المستخدم ويمكن أن تشمل بيانات المتصفح، والجهاز الذي يستخدمه، وبيانات الموقع الجغرافي، وما يبحث عنه عبر محركات البحث، وتفضيلاته، وغير ذلك، واستخدامها من أجل الحصول على بيانات استدلالية وبناء ملفات شخصية للمستخدم. فإذا تعمّد المستخدم إعطاء بيانات وهمية أو غير صحيحة فإن ذلك يُعدّ - في الأغلب- غير وارد بالنسبة للبيانات التي تشكل البصمة السلبية (فعلى سبيل المثال، إذا ادعى شخص وجوده في مكان آخر غير المكان الذي به الآن، وقدم من خلال ذلك معلومات زائفة ضمن بيانات بصمته الإيجابية أو النشطة، فمن غير الممكن بصورة كبيرة خداع البرمجيات التي بإمكانها معرفة مكانه الحالي، وتمثل بذلك بصمته السلبية أو غير النشطة).

أما مفهوم الملكية المشتركة أو الوصاية على البيانات فيتوقع المستخدم أن عند إخباره بمعلومات - يعني إمكان أن يمتلكها آخرون- يحمل التزاماً للمستلم بأن المعلومات محمية وفقًا لرغبات المالك الأصلي، ولا تُستخدم بشكل آخر غير ما صرَّح له بها (كأن تُستخدم في الحصول على معلومات استدلالية يبنى من خلالها ملفات شخصية للمستخدم، أو أن تحمل التزاماً فيما يتعلق بنشر معلوماته ومشاركتها مع طرف ثالث). وعندما لا يتفاوض مالكو المعلومات بشكل فعَّال ولا يتبع المالكون المشتركون التزام الخصوصية الضمنية؛ يحتمل أن يظهر اضطراب حدودي نتيجة لذلك. وفي سياق الاتصالات المعتمدة على الإنترنت، فإن واقع المنافع الذي يسهم في خلق بعض الفوائد الإيجابية العائدة من منح بياناتهم لهذه الجهات قد ينتج عنه اضطراب أثناء تقييمهم للمخاطر مقابل المنافع. وفي هذا الإطار تستكشف الدراسة أحد عناصر النظرية الأساسية، ويتمثل في الملكية والتحكم؛ إذ تهدف إلى معرفة وجهة نظر المستخدم في ملكية البيانات واعتقاده عن الجهات التي تجمع بياناته من خلال مجموعة من التساؤلات الاستكشافية **ومقياس (إدارة البصمة الرقمية)**.

**تساؤلات الدراسة:**

1- ما مدى معرفة المستخدمين بالبصمة الرقمية والأنشطة الرقمية التي تؤدي لتشكيلها؟

2- ما مستوى حساسية بعض المعلومات الخاصة لدى المستخدمين؟

3- ما المدة الزمنية التي يعتقد المستخدم أنه ينبغي على شركات التكنولوجيا والاتصالات الاحتفاظ فيها ببياناته؟

4- ما مدى معرفة المستخدمين بالمنافع المتصورة للبصمة الرقمية؟

5- ما مدى معرفة المستخدمين بالمخاطر المتصورة للبصمة الرقمية؟

6- كيف يُتخذ القرار بحماية البصمة الرقمية؟

7- ما مستوى تحكم المستخدم في البصمة الرقمية؟

**فروض الدراسة:**

الفرض الأول: توجد علاقة ارتباطية بين مستوى الوعي بالبصمة الرقمية وفقًا للمتغيرات الديموغرافية (النوع والعمر).

الفرض الثاني: توجد علاقة ارتباطية دالة إحصائيًا بين مستوى المعرفة بالأنشطة المكونة للبصمة الرقمية وفقًا للمتغيرات الديموغرافية (النوع والعمر).

الفرض الثالث: توجد علاقة ارتباطية دالة إحصائيًا بين مستوى إدارة بالبصمة الرقمية لدى المبحوثين وفقًا للمتغيرات الديموغرافية (النوع والعمر).

الفرض الرابع: توجد علاقة ارتباطية بين وعي المستخدمين بالبصمة الرقمية ومستوى إدارة البصمة الرقمية.

**الإجراءات المنهجية للدراسة:**

**نوع الدراسة ومنهجها:** تعد الدراسة من الدراسات الوصفية التي تهدف إلى رصد الظواهر ووصفها بشكل يُمكِّن من تفسير الخصائص والسلوكيات والظروف المحيطة بها، وقد اعتمدت الدراسة على منهج المسح الكمي بوصفه أنسب المناهج للدراسات الوصفية؛ كونه منهجًا كميًا يهدف إلى القياس الإحصائي لمتغيرات الدراسة بما يمكن من وصفها وتفسيرها.

**مجتمع الدراسة واختيار العينة:** يتحدد مجتمع الدراسة في مستخدمي الإنترنت بجمهورية مصر العربية، الذين وصل عددهم لأكثر من ٨٣ مليون مستخدم وفقًا للنشرة الربع سنوية (يناير – مارس ٢٠٢٣) لمؤشرات الاتصالات وتكنولوجيا المعلومات الصادرة عن وزارة الاتصالات وتكنولوجيا المعلومات، فقد وصل عدد مستخدمي الإنترنت إلى ما يقرب من ٨٣.٧ مليون مستخدم على النحو: (٦٩.٨٦) مشترك عن طريق الهاتف المحمول، و(٢.٥٢) مليون مستخدم عن طريق (USB Modem)، و(١١.٣٢) مليون وصلة للإنترنت فائق السرعة.

وقد اعتمدت الدراسة على العينة العمدية من مستخدمي الإنترنت بجمهورية مصر العربية، ولتحديد حجم العينة اعتمدت الباحثة على معادلة "ستيفن ثامبسون"(54) لحساب حجم العينة على النحو الآتي:

$$n = \frac{NP(1-P)}{(N-1)\ (d^2/z^2) + P(1-P)}$$

حيث: N ترمز لحجم المجتمع، وZ تعني الدرجة المعيارية المقابلة لمستوى الدلالة 0.95 وتساوي 1.96، وd ترمز لنسبة الخطأ وتساوي 0.05، وp هي نسبة توفر الخاصية والمحايدة = 0.50. وبتطبيق المعادلة على حجم المجتمع ٨٣.٧ مليون مستخدم تكون حجم العينة ٣٨٤.١٥ أي ٣٨٥ بالتقريب.

**جدول (١) توصيف العينة**

| المتغير | المجموعات | ك | % |
|---|---|---|---|
| الفئة العمرية | أقل من ٢١ سنة | 88 | 22.9% |
| | من ٢١ سنة إلى أقل من ٣٠ سنة | 114 | 29.6% |
| | من ٣٠ سنة إلى أقل من ٤٠ سنة | 108 | 28.1% |
| | ٤٠ عاماً فأكثر | 75 | 19.5% |
| النوع | أنثى | 236 | 61.3% |
| | ذكر | 149 | 38.7% |
| المستوى التعليمى | طالب في المرحلة الجامعية | 151 | 28.2% |
| | حاصل على مؤهل متوسط | - | - |
| | حاصل على مؤهل عال | 109 | 54.35 |
| | دراسات عليا | 25 | 6.5% |
| متوسط الدخل الشهري للأسرة | أقل من ٤٠٠٠ جنيه | 39 | 10.1% |
| | من ٤٠٠٠ إلى أقل من ٨٠٠٠ | 104 | 27% |
| | من ٨٠٠٠ إلى أقل من ١٢٠٠٠ | 159 | 41.3% |
| | ١٢٠٠٠ فأكثر | 83 | 21.6% |
| | **الإجمالى** | 385 | 100% |

**أداة جمع البيانات:**

في إطار اعتماد الدراسة على المسح بالعينة، من أجل توصيف معرفة المستخدمين بالبصمة الرقمية وتشكيلها وتأثيراتها ومستوى التحكم فيها، اعتمدت الدراسة على أداة

الاستبانة لجمع البيانات من عينة الدراسة، فاعتمدت على صحيفة الاستقصاء الإلكتروني، وتوزعت أسئلة الاستقصاء على عدة محاور: المحور الأول: البيانات الديموغرافية وأشكال الاستخدامات الرقمية للمبحوثين، المحور الثاني: حساسية بعض المعلومات بالنسبة للمستخدم، المحور الثالث: حول مفهوم البصمة الرقمية والأنشطة التي تعمل على تشكيلها، المحور الرابع: تأثيرات البصمة الرقمية، المحور الخامس: أسلوب اتخاذ القرار ومستوى التحكم في البصمة الرقمية. وقد أُتيح الاستقصاء للجمهور خلال الفترة الزمنية (١٥ سبتمبر حتى ٣٠ أكتوبر ٢٠٢٣).

**صدق الاستمارة وثباتها:**

تأكدت الباحثة من صدق الاستبانة وأنها تقيس ما ينبغي قياسه، وأن الأسئلة تعكس أهداف الدراسة وتساؤلاتها، وذلك بقياس صدق الاستمارة بعرضها على مجموعة من المُحكِّمين[55] للتحقق من مصداقيتها وشمولها، وأنها تقيس بالفعل ما استهدفته الدراسة، وفي ضوء ملاحظاتهم عُدِّلت الاستمارة. أما ثبات الاستمارة فقد كان بحساب معامل ثبات ألفا كرونباخ لاستجابات العينة، وبلغت نسبته 0.897، وهي نسبة ثبات مقبولة إحصائيًا.

**المعالجة الإحصائية للبيانات:**

عالجت الباحثة البيانات إحصائيًا بالاعتماد على برنامج ( Statistical Package for the Social Sciences) SPSS، لملاءمته لطبيعة الدراسة وقدرته على تكوين الجداول التكرارية وإيضاح العلاقات بين المتغيرات، وذلك بحساب التكرارات ونسبها المئوية في الجداول السيطة، وحساب كل من المتوسط الحسابي والانحراف المعياري والوزن النسبي للمقاييس، وإيجاد قيمة (ت) للاستدلال على الفروق بين متوسطات درجات العينة في مقاييس الدراسة، إضافة إلى حساب معامل ارتباط بيرسون لقياس الارتباط بين المتغيرات.

**البصمة الرقمية.. المفهوم والأنواع:**

تتعدد المصطلحات التي تشير إلى البصمة الرقمية، فقد استخدمت بعض الأدبيات السابقة مصطلح Digital Footprint، ومصطلح Digital Trial، ومصطلح Digital Breadcrumbs، وبصفة عامة، يُجمع الباحثون على أن مفهوم البصمة

الرقمية يشير إلى المعلومات والبيانات التي يخلفها الأفراد خلفهم في العالم الرقمي من خلال إجراءات يقومون بها بشكل إيجابي هادف (مقصود)، أو أفعال سلبية (غير مقصودة)(56)، فالاستخدام المستمر للأجهزة الرقمية يترك وفرة من البيانات تحتوي على معلومات عن أنشطة الأفراد، كأماكن وجودهم، أو مشترياتهم، أو اهتماماتهم، أو جهات الاتصال لديهم... إلخ(57)، والرسائل والصور التي يتم تحميلها، أو البيانات الوصفية المتعلقة بالوسوم التي يتم النقر عليها في مواقع الويب(58).

وكثيرا ما يكشف البحث السريع عبر الإنترنت عن قدر كبير من المعلومات الشخصية، بما في ذلك تفاصيل الاتصال بنا، وأماكن وجودنا، والعائلات، والعلاقات، والآراء السياسية... إلخ، ويشار عادة إلى استخدام هذه المعلومات لأغراض خبيثة باسم Doxing، ففي معظم الحالات تكون المعلومات غير ضارة، ولكن في الحالات الأكثر خطورة يمكن استخدام هذه المعلومات لتشويه سمعة الأفراد أو استهدافهم، وكان هذا هو الحال في أعقاب محاولة الانقلاب في تركيا؛ فقد شاركت السلطات في تطهير واسع للأكاديميين والصحفيين والناشطين(59). وقد استخدم علماء الكمبيوتر البيانات الرقمية للتنبؤ بنجاح الأحداث، مثل (انتشار الأنفلونزا في الولايات المتحدة، وإيرادات شباك التذاكر للأفلام الجديدة، ونتائج الانتخابات، وردود الأفعال أو الآراء لأحداث مثل الربيع العربي)(60). وعلى الرغم من استخدام كثيرين للإنترنت فإنهم لا ينظرون بوعي لتأثير استخدامهم للإنترنت في هويتهم الرقمية مع تركيزهم على الفوائد قصيرة المدى، مثل القدرة على التواصل مع الأصدقاء، فعلى الجانب الآخر ليس فقط بإمكانك العثور على ما تبحث عنه عن الآخرين؛ إذ يمكن لهم أيضًا الحصول على المعلومات نفسها عنك(61).

**وتنقسم أنواع البصمة الرقمية الأساسية إلى بصمة رقمية نشطة وأخرى سلبية:**
البصمة الرقمية النشطة Active Digital Footprint تعني الإجراءات المتعمدة للمستخدم على الإنترنت والمنصات الرقمية، على سبيل المثال: منشور ينشره على حساب الشبكات الاجتماعية الخاصة به، أو رسالة بريد إلكتروني أرسلها، وبالنظر إلى استخدام شبكات مثل Twitter وFacebook وInstagram وSnapchat، تظهر كميات

كبيرة من البيانات في عمليات إنتاج واستهلاك هذه الشبكات، فتكون مسؤولية ونتائج هذه الإجراءات الرقمية شخصية(62)، بمعنى أنها تأتي من المستخدمين أنفسهم بشكل مقصود عندما يعرضون بياناتهم الخاصة بكامل إدراكهم لما يمكن للآخرين رؤيته عنهم، مثل بياناتهم الشخصية، ومكان وجودهم، وصورهم، وآرائهم... إلخ. ويمثل هذا النوع من البصمة النشاط الجيد والسيئ للفرد؛ أو الصورة الحسنة الجيدة وغير الجيدة عنه بحسب ما يظهر نفسه للآخرين، أي ما يتعلق بالسمعة، وهو ما يتمتع الفرد بالقدرة على تشكيله وبنائه والتخطيط له بشكل لا تستطيع الأنواع الأخرى من البصمات فعله. فمثلًا، يُنشئ المستخدمون بموقع لينكدإن LinkedIn هذه البصمات الرقمية النشطة عبر بياناتهم في الملف الشخصي والكشف هويتهم والتعبير عنها لأغراض مختلفة، مثل التطوير الوظيفي، ويمكن ملاحظة هذه البصمات الرقمية النشطة من قبل مستخدمين آخرين، مثل مسؤولي التوظيف أو الأفراد الذين يبحثون عن آخرين في التخصص ذاته، مما يعني أنه يمكن للمستخدمين الاستعانة بها بصورة عمدية للتعبير عن أنفسهم بشكل إيجابي لأهداف مثل صياغة هويتهم لجذب الشركاء المحتملين.

وقد لا يمكن الوصول إلى بعض البصمات الرقمية النشطة، مثل تلك التي تُنشأ على شبكات التواصل الاجتماعي دون إذن المستخدم بناء على مستوى الأمان في حساب الوسائط الاجتماعية، فعلى الرغم من أن منصات التواصل الاجتماعي تحاول الحفاظ على خصوصية المستخدم، فإن بعض أجزاء ملفات تعريف المستخدمين عادة ما تكون عامة بمعرفة المستخدم وبإذنه.

البصمة السلبية Passive Digital Footprint: يصف الباحثون شكلين من أشكال المشاركة السلبية: الأول هو "المنتج الثانوي" التشاركي الذي تولده الخوارزميات على أساس سلوك المستخدمين على الإنترنت، أي البيانات التي يخلفها المستخدم خلفه دون قصد أو دون وعي منه أنه ترك هذه البيانات، ويمكن أن يتضمن التصفح العشوائي، والإعجاب(63)، وتسجيل مواقع الويب التي يزورها المستخدم لعنوان IP الخاص به، وتفصح عن معلومات الموقع الجغرافي(64)، فعنوان IP الخاص بالمستخدم قد لا يتضمن أي بيانات شخصية، كما أنه قد يتغير إلا أنه يظل جزءاً من البصمة الرقمية

للمستخدمين، كما يمكن معرفة مُزوِّد خدمة الإنترنت للمستخدم. علاوة على ذلك، تحتفظ محركات البحث بسجل بحث المستخدم وتفضيلاته، ويمكن التعرف عليها من خلال حساب المستخدم، ويعني ذلك أن البصمة السلبية تتشكل نتيجة عمليات يفرضها النظام دون إرادة المستخدم وخارج سيطرته، ولا يمكن التحكم فيها، وتكون إثر التفاعل مع البنية الإلكترونية فتنتج مدخلات في سجلات المواقع، أي أنها غير طوعية الإفصاح، ولا يوجد تدخل متعمد من الشخص في الإفصاح عنها، فكل زيارة لموقع وكل عملية بحث يجريها تُخزَّن في قواعد بيانات وقد تُحلَّل لأغراض متعددة.

أما الشكل الثاني من السلوك السلبي فهو ذلك الذي يشارك فيه المستخدمون "الآخرون" في أنشطة مثل وضع العلامات أو الإشارة إلى الآخرين Tagging، والتعليق تجاه الفرد أو المجموعة محل التركيز، ويعني ذلك أن حصة مهمة من البيانات الشخصية عبر الإنترنت مستمدة من "المشاركة السلبية"، وهي الآثار التي يطلقها المستخدمون عن غير قصد، حتى من قبل مستخدمين آخرين أيضًا أثناء تجاربهم عبر الإنترنت(65).

وأطلق بعض الباحثين على النوع الثاني من البيانات السلبية- البيانات التي يُنشئها آخرون عن المستخدمين- مصطلح ظلال البيانات الرقمية Digital Shadows. ومما لا شكَّ فيه أن المعلومات التي تُنتج على مدى سنوات لا تنشأ بشكل نشط بواسطة الأشخاص أنفسهم فحسب، بل تنشأ أيضًا من خلال آثار ينشئها الآخرون عنهم، وقد تتفوق آثار "الظل الرقمي" الخاص بالأفراد على البصمة الرقمية النشطة التي ينشئها بنفسه(66). كما أطلق عليه بعض الباحثين مسمى Second-Hand Digital Footprint، الذي انتشر بعد تطور الويب وازدهار مواقع التواصل، وقد تكون هذه البيانات حول سلوك الأفراد على الإنترنت أو خارج الإنترنت، كأن تكتب مقالًا في نسخة مطبوعة وينشره أحد الزملاء على مدونته أو على صفحته بمواقع التواصل الاجتماعي، أو تتمثل في مقاطع الفيديو أو الصور التي تنشر دون إذن الأفراد لتعرض حدثًا قد يكون إيجابيًا أو سلبيًا(67).

**إنترنت الأشياء واتساع البصمة الرقمية للمستخدمين:**

لقد أصبحنا نعيش في عصر إنترنت الأشياء (IoT)، وباتت جميع الأشياء ذكية؛ هواتف ذكية، وساعات ذكية، وسيارات ذكية، ومنازل ذكية، ومبانٍ ذكية... وغيرها كثير، وزاد الاعتماد على استخدام البيانات البايوميترية (القياسات الحيوية)، على سبيل المثال لفتح الأبواب؛ إذ يتعين على المستخدمين استخدام التعرف على الصوت أو بصمات الأصابع، أو التعرف على الوجه لاستخدام الجهاز، وتُخزّن هذه البيانات في خادم متصل بالشبكة، لذلك تمثل هذه البيانات مسارات رقمية أو بصمة رقمية. كما أن أحد الطرق الشائعة التي تسهم بها المباني في البصمة الرقمية استخدام كاميرات الدوائر التلفزيونية المغلقة، التي تكون إما متصلة عبر الإنترنت، أو ضمن شبكة محلية؛ إذ ترسل الكاميرات باستمرار فيديو المراقبة الرقمي إلى الخوادم، وبذلك يحظى رواد المبنى ببصمة رقمية. وتسهم الهواتف المحمولة أيضًا في المسارات الرقمية، فالمستخدمون يميلون إلى تنزيل عديد من التطبيقات على هواتفهم دون فهم كيفية اتصال هذه التطبيقات بالإنترنت، أو البيانات التي تُجمع وتُخزَّن، لأن مُطوِّر التطبيق يكون مسؤولاً عن التحكم في كيفية إرسال التطبيق أو استقباله للبيانات من وإلى الأجهزة والخدمات الأخرى، التي لا يملك المستخدم سوى القليل من التحكم فيها، أو لا يتحكم فيها على الإطلاق(68). ويعني ذلك أن أجهزة إنترنت الأشياء تعمل على زيادة المسارات الرقمية لعديد من المستخدمين بسرعة، ويعتمد الجيل الجديد من أجهزة إنترنت الأشياء على البيانات، ولكن بما أنها قد تبدو فعالة وموثوقة، فإنها تترك وراءها عديدًا من الآثار الرقمية.

**تفاوت المسارات الرقمية وتأثيرات البصمة الرقمية:**

بصفة عامة، تعني الفجوة الرقمية عدم المساواة الاجتماعية والاقتصادية في الوصول للإنترنت والاندماج في أنشطتها، فهو أحد مظاهر الإقصاء الرقمي والتمايز المباشر، أما الفجوة في البصمة الرقمية، أو ما يمكن تسميته تفاوت المسارات الرقمية، فيمكن إرجاعه لعدة أمور؛ فقد استخدم بعض الباحثين مثل (Büchi, M. et al. 2017)، (Büchi, M. 2017)، (Robinson, L. 2015) مصطلح (تفاوت المسارات الرقمية، أو الفجوة الرقمية) عند الحديث عن عدم المساواة الرقمية، سواء في سياق مقدار الآثار التي يتركها الأشخاص عند استخدامهم صفحاتهم الشخصية أو صفحات المجموعات، أو

مظاهر البصمة الرقمية للأطفال حين يبث آباؤهم الحياة اليومية لهم دون معرفتهم أو موافقتهم لعدم أهليتهم للاختيار، ويتوسع المفهوم ليأخذ في الاعتبار ليس فقط مقدار البصمة الرقمية التي شُكِّلت؛ لكنه يشمل مظاهر عدم المساواة في الخلفيات الاجتماعية والاقتصادية والثقافية المختلفة للأفراد، التي تمكنهم من القدرة على إدارة بصماتهم، واعتبار عدم المساواة الاجتماعية سبب الفروق في الاستخدامات والمهارات(69). لذلك يمكن القول إن التوعية ذات أهمية بالغة لتنمية الوعي فيما يتعلق بإدارة البصمة الرقمية على المدى الطويل؛ إذ تُعدّ بمثابة الكفاءة الأساسية للوجود عبر الإنترنت والثقافة التشاركية.

ورغم أن البصمة الرقمية قد تبدو أحد الجوانب السلبية لنشاط المستخدم عبر الإنترنت؛ إذ يُحتفظ ويُدوَّن كل نشاط له، سواء من خلال البصمة الرقمية النشطة أو السلبية، فإن للبصمة الرقمية عديدًا من المزايا يُمكن أن تساعد على جعل تجربة الفرد عبر الإنترنت أكثر نفعًا ودقة وسهولة، فعلى سبيل المثال، يستخدم Google Adsense البصمة الرقمية السلبية الخاصة بنا لتخصيص الإعلانات، إلا أنه قد حصل على الإذن منا بجمع بياناتنا في وقت التسجيل، لأن شروط وسياسات الاستخدام تذكر أنهم سيستخدمون بيانات تصفح الويب الخاصة بنا لتقديم إعلانات أكثر ملاءمة وفقًا للمحتوى الذي نبحث عنه، فمثلًا: يستخدم يوتيوب YouTube بصمتنا الرقمية لتحسين قائمة مقاطع الفيديو ذات الصلة، كما يستخدم فيسبوك أيضًا البصمة الرقمية لمنحنا تجربة أفضل للتواصل الاجتماعي من خلال عرض الإعلانات وفقًا لإعجاباتنا وإعجابات الأصدقاء، كما يعرض قائمة الأصدقاء المقترحة وفقًا لقائمة الأصدقاء وقائمة الأصدقاء المشتركين... إلخ(70).

بينما يتمثل أبرز عيوب البصمة الرقمية في جمع البيانات حول نشاط المستخدم عبر الإنترنت دون وعيه ومعرفته، خاصة في البصمة الرقمية السلبية، وعادة ما نزور أنواعًا مختلفة من مواقع الويب، ونستخدم تطبيقات بشروط وأحكام مختلفة تكون طويلة جدًا عند قراءتها، وفي معظم الأوقات نوافق على الشروط والأحكام دون حتى قراءتها ونبدأ في استخدام موقع الويب والخدمات، مما يؤدي إلى منح الحقوق القانونية لموقع

الويب لجمع معلومات النشاط عبر الإنترنت، لذا يجب على المستخدم التسلح عبر الفهم والمعرفة لمفهوم البصمة الرقمية، والبيانات التي قد تُخزِّنها المواقع التي يزورها، فيستطيع تحديد كيفية حماية بياناته والإبحار بأمان على الشبكة.

والواقع أن لدى جميع المستخدمين بصمة رقمية، سواء رغبوا في ذلك أو لا؛ وتعد البيانات التي تُجمع عن الأفراد متاحة، ليس فقط لأنفسهم، إنما تُجمع وتُخزَّن بطريقة مركزية بواسطة شركات الإنترنت، مثل جوجل أو أبل أو فيسبوك، وقد لا تُستخدم هذه البيانات لخدمة مصالح الأفراد؛ إذ تتحكم فيها كيانات أخرى لها اهتمامات مختلفة أحيانًا عن اهتمامات الفرد؛ وقد لا يعرف الأشخاص ما البيانات التي تُجمع وتُخزَّن؛ وقد تتبادل الشركات بيانات الأفراد(71).

وبينما تعد البصمة الرقمية النشطة الأكثر قابلية للتحكم من قبل المستخدم؛ إلا أنه قد لا يحسن تطويعها بشكل إيجابي، فتظهر سمعة رقمية سلبية، فمن التأثيرات المهمة التي يمكن الإشارة إليها التأثير في مستقبله الوظيفي أو فرص العمل المستقبلية بعد أن أصبحت البصمة الرقمية معياراً للتقييم، كما أصبحت شائعة الاستخدام في المراقبة، فتشير إحدى المقالات إلى أنه وفقًا لمسح التوظيف الاجتماعي فإن حوالي ٩٣% من المختصين بتعيين الموظفين يدققون في الملفات الشخصية للمرشحين للوظيفة قبل أن تعيينهم، وأن حوالي ثلث أصحاب العمل، البالغ عددهم ٢٣٠٠ شخص، شاركوا في استطلاع للرأي أجراه موقع CareerBuilder.com، وجدوا محتوى على مواقع التواصل الاجتماعي أدى إلى عدم منح المرشح عرض العمل لأسباب مختلفة، منها (وضع صور استفزازية أو غير لائقة – ضعف في مهارات الكتابة – إهانة مديرين سابقين – تعليقات عنصرية – الكذب حول مؤهلات الشخص)(72). وتفصل بعض القصص الإعلامية الحالات التي فقد فيها الأفراد وظائفهم أو رفض قبول طلاب بالجامعات استنادًا إلى المحتوى المنشور في حساباتهم على مواقع التواصل الاجتماعي، فيشير تقرير منشور على جريدة "نيويورك تايمز" إلى أن نسبة كبيرة من المختصين بقبول الطلاب بالجامعات دققوا في ملفاتهم عبر مواقع التواصل الاجتماعي لمعرفة مزيد عنهم، وأن حوالي ٣٠% من المختصين توصلوا إلى معلومات أثَّرت سلبًا في قبول هؤلاء

الطلاب(73). وتشير دراسة لـ (ExecuNet) إلى أن حوالي ٧٧% من العاملين في مجال التوظيف أفادوا بأنهم استخدموا محركات البحث للعثور على بيانات أساسية عن المرشحين للعمل، وأفاد ٣٥% منهم بأنهم رفضوا مرشحين بسبب ما عثروا عليه عنهم عبر الإنترنت(74). وقد أصبحت أمثلة الطرد من الوظيفة بسبب منشورات الفرد على شبكات التواصل الاجتماعي شائعة، لذلك ينبغي أن يعيي الأفراد كيفية إنشاء بصمة إيجابية من أجل تعظيم فرصهم الوظيفية وسمعتهم الرقمية التي تعد امتداداً لسمعتهم في الواقع.

وتمثل الحالات السابقة مثالًا لتأثيرات سيئة للبصمة الرقمية النشطة التي نشرها المستخدم عن نفسه، ولما كانت هذه الاحتياجات الرقمية، مثل مواقع التواصل الاجتماعي والخرائط وإنترنت الأشياء، والأجهزة مثل الهواتف المحمولة والأجهزة اللوحية، أدوات تُمكِّن الأشخاص من مشاركة تجاربهم اليومية بسهولة عبر الصور ومقاطع الفيديو والقصص... وغير ذلك، ولما كان من الصعب العمل بعيداً عن كل هذه التقنيات، أصبح من المهم أن يتحكم الفرد في البصمة الرقمية ليبدو إيجابياً، عبر تجنب الإفراط في المشاركة على منصات التواصل الاجتماعي، ومحاولة القيام بدور العكسي والبحث عن أنفسهم لمعرفة ماذا قد يجد الآخرون عنهم.

**إنفاذ قواعد حماية البيانات والحق في النسيان:**

من المؤكد أن الاتجاهات التكنولوجية الحالية، مثل الحوسبة السحابية والشبكات الاجتماعية، وكذلك عولمة تدفق البيانات، تهدد بتلاشي المبادئ الأساسية للخصوصية، واستحداث عصر التذكر المثالي Perfect Remembering؛ مما أدى إلى إحداث تحولات عميقة في طريقة معالجة البيانات الشخصية واستخدامها والتصميم على إنفاذ قواعد لحماية البيانات، وإدراك الحاجة إلى تحديث تنظيم البيانات و(الحق في النسيان) Right to Be Forgotten، أو الحق في الشطب Right to Erasure(75).

فبينما يثير دور الخوارزميات في معالجة المعلومات الاجتماعية جدلًا حول عواقب الرقمنة على التذكر "ذاكرة الويب"، فغالبًا ما ترتبط الخوارزميات بتوسع غير مسبوق في التذكر، الذي يُعبَّر عنه من خلال فكرة واسعة الانتشار مفادها أن "الإنترنت لا ينسى

أبدًا"، لأن البيانات المُخزَّنة في الأرشيفات الرقمية يمكن إتاحتها تلقائيًا من خلال محركات البحث، إلا أن الحاجة إلى النسيان أمر أكثر أهمية من القدرة على التذكر؛ فدون النسيان، سيظل المرء مقيدًا بالحضور الأبدي للماضي، وهو ما لا يسمح ببناء مستقبل مختلف(76).

وكانت لجنة وزراء مجلس أوروبا قد أوصت في وقت سابق في التوصيات (٥/٩٩)، بعنوان "حماية الخصوصية على الإنترنت" بمجموعة من القواعد الإرشادية لمستخدمي الإنترنت، ودعتهم للحذر والعمل على تحسين حماية بياناتهم نظرًا لاعتبار الإنترنت مكانًا غير آمن، فأوضحت أن كل معاملة يقوم بها المستخدم، وكل موقع يزوره على الإنترنت، تترك آثارًا إلكترونية، ويمكن استخدامها دون علمه من أجل إنشاء ملف تعريف يحدد شخصيته واهتماماته، كما أشارت إلى أن إخفاء الهوية بالكامل أمر من الصعب تحقيقه (على سبيل المثال: إذا جاز لك استخدام اسم مستعار ستبقى هويتك الشخصية معروفة لمزود خدمة الإنترنت الخاص بك)، كما أوصت بإعطاء مزود خدمة الإنترنت أو أي شخص آخر فقط البيانات اللازمة لتحقيق غرض محدد تم إعلامك به. كما لم تغفل التوصية لمقدمي الخدمات بضمان سلامة البيانات وسريتها، وضرورة إعلام المستخدمين بمخاطر الخصوصية، مثل جمع البيانات أو تسجيلها بشكل مخفي، وضرورة إعلام المستخدمين بالوسائل التقنية التي قد يستخدمونها بشكل قانوني لتقليل المخاطر الأمنية على البيانات والاتصالات، مثل التشفير المتاح قانونيًا والتوقيعات الرقمية. وإعلام المستخدمين بالبرامج التي تتيح لهم البحث والتصفح بشكل مجهول على الإنترنت، وتصميم نظامهم بطريقة تتجنب أو تقلل من استخدام البيانات الشخصية، وعدم جمع ومعالجة وتخزين البيانات المتعلقة بالمستخدمين إلا عند الضرورة بشكل صريح ومحدد وعدم تبادل البيانات، وعدم تخزين البيانات لفترة أطول مما هو ضروري لتحقيق غرض المعالجة، وعدم استخدام البيانات لأغراض ترويجية أو تسويقية إلا إذا لم يعترض الشخص المعني، بعد إبلاغه بذلك، أو في حالة معالجة بيانات المرور أو البيانات الحساسة قد أعطى موافقته الصريحة، كما ألزمتهم بالمسؤولية عن الاستخدام السليم

للبيانات، وتسليط الضوء حول سياسة الخصوصية قبل أن يبدأ المستخدم في استخدام الخدمات(77).

وقدمت مبادرة قانون الاتحاد الأوروبي لإنفاذ اللائحة العامة لحماية البيانات فصلًا جديدًا لحماية الخصوصية المعلوماتية في أوروبا واجب التطبيق اعتباراً من أغسطس ٢٠١٨؛ ليحل محل قانون حماية البيانات الذي صدر عام ١٩٩٨ ليلائم بصورة أكبر التطورات الخاصة بالبيانات، وهي مجموعة من القوانين وُضعت للسماح للأفراد بالتحكم في بياناتهم الشخصية، ومن ثم لن تتمكن الشركات من الحصول على أي بيانات دون إذن المستخدم، ووفقًا للمادة (١٧) من هذا القانون، يمكن أيضًا للأفراد محو البيانات الشخصية(78)، وهو يعد واحدًا من أقوى القوانين الخاصة بالبيانات في العالم، وأكثر ديناميكية، ويفرض غرامات صارمة على الشركات التي تُسرِّب البيانات الشخصية.

وكانت محكمة العدل التابعة للاتحاد الأوروبي قد أصدرت قراراً في مايو ٢٠١٤ في القضية التي تقدم فيها المواطن الإسباني (ماريو كوستيا) بشكوى إلى وكالة حماية البيانات الإسبانية، ضد صحيفة Vanguardia وشركة جوجل ومحرك بحث جوجل إسبانيا، فيما يتعلق بصفحات من الصحيفة ظهرت في نتائج بحث جوجل عند البحث عن اسمه (احتوت الصفحة على إعلان عن مزاد عقاري في أعقاب إجراءات استرداد الضمان الاجتماعي المستحقة عليه)، ورفضت المحكمة الدعوى المقامة ضد الصحيفة، لأن المعلومات نُشرت بشكل قانوني، بينما أيدت الشكوى ضد شركات جوجل وطلبت اتخاذ الإجراءات اللازمة لسحب البيانات من فهارسها، وقد فُسِّرت الأحكام بالاستناد إلى الحق في النسيان على الشبكة(79).

وبدأت شركات التكنولوجيا مؤخراً النظر إلى خصوصية المستخدم كشيء يجب تقديره، ففي عام 2020، على سبيل المثال، وضعت Google خطة من أجل "شبكة ويب أكثر خصوصية"؛ إذ ستتوقف عن دعم ملفات تعريف الارتباط التابعة لجهات خارجية واستخدام تقنية صندوق الرمل Privacy Sandbox (تقنية من شأنها التحكم في ظهور المواقع الحديثة والناشئة، وعدم ظهورها في نتائج محرك البحث إلا بعد فترة زمنية من اختباره، والتأكد من محتواه وجودته قبل إتاحة عرضه للمستخدمين).

**نتائج الدراسة:**

**جدول (٢) عدد ساعات استخدام الإنترنت**

| عدد ساعات استخدام الإنترنت | ك | % |
|---|---|---|
| أقل من ساعة يومياً | - | - |
| من ساعة إلى أقل من ٣ ساعات | 105 | 27.3% |
| من ٣ ساعات إلى أقل من ٥ ساعات | 190 | 49.4% |
| ٥ ساعات فأكثر | 90 | 23.4% |
| **الإجمالى** | 385 | 100% |

تدلل نتائج الجدول السابق (٢) على زيادة الاعتماد على الإنترنت في حياة الأفراد اليومية بصورة كبيرة، فمعظم أفراد العينة بنسبة ٤٩.٤% ينخرطون في استخدام الإنترنت لفترة تتراوح بين ٣ ساعات إلى أقل من ٥ ساعات على مدار اليوم، بينما ٢٧.٣% يستخدمون الإنترنت يومياً ما بين ساعة إلى أقل من ٣ ساعات، وفي المقابل فإن ٢٣.٤% يستغرقون مدداً زمنية أطول تصل إلى أكثر من ٥ ساعات في اليوم، ويلاحظ أنه رغم إتاحة خيار "أقل من ساعة يومياً" للجمهور فإن استجابتهم تجاه هذا البديل كانت منعدمة.

وتختلف هذه النتيجة جزئياً مع نتائج دراسة (محمود محمد، ٢٠٢٢)(80)، التي أشارت إلى أن معدل الاستخدام اليومي لشبكة الإنترنت أكثر من ٥ ساعات، يليه من ٣ إلى ٥ ساعات.

وترجع الباحثة هذه النتيجة إلى العوامل التي أدت إلى مزيد من الاعتماد الرقمي، ومنها: تغير أساليب التواصل والاتصال بين الأفراد، سواء عبر شبكات التواصل الاجتماعي أو تطبيقات المحادثة، واتجاه أساليب الترفيه المتنوعة إلى الرقمنة، سواء عبر مشاهدة الفيديوهات والبرامج أو المنصات الترفيهية والألعاب الإلكترونية، إضافة إلى الاعتماد على المنصات المختلفة المساعدة في البحث عن المعلومات، والتعلم عن بُعد، وخدمات البث المباشر، والمؤتمرات الافتراضية، وغير ذلك من الاستخدامات المختلفة. وجميع هذه الاستخدامات كان نتيجة طبيعية لإتاحة خدمات الإنترنت وجعلها في متناول

الأفراد، وكذلك توافر الوسائل الوسيطة المستخدمة للوصول إلى الإنترنت وأهمها الهواتف الذكية في أيدي الجمهور، إضافة إلى التطورات المستمرة في عالم تكنولوجا الاتصالات، وتمثل ذلك جميعه في فترات استخدام طويلة للإنترنت على مدار اليوم.

**جدول (٣) أكثر الأجهزة الرقمية التى يستخدمها المبحوثون**

| الأجهزة التى تستخدمها باستمرار | ك | % |
|---|---|---|
| حاسوب مكتبي | 19 | 4.9% |
| جهاز لوحي (لابتوب) | 236 | 61.3% |
| هاتف ذكي | 341 | 88.6% |
| تابلت | 116 | 30.1% |
| ساعة ذكية | 109 | 28.3% |
| تليفزيون ذكي | 195 | 50.6% |
| أجهزة الألعاب الذكية (كونسول) مثل بلايستيشن – إكس بوكس | 71 | 18.4% |
| الأجهزة القابلة للارتداء (أساور تتبع اللياقة البدنية) | 51 | 13.2% |
| ن = ٣٨٥ | | |

تشير نتائج الجدول (٣) إلى أكثر الأجهزة التي يعتمد عليها المبحوثون، وكان الهاتف الذكي أكثر الأجهزة استخداماً لدى ٨٨.٦% من أفراد العينة، يلي ذلك الاعتماد على استخدام الكمبيوتر المحمول بنسبة ٦١.٣%، ثم التليفزيون الذكي بنسبة ٥٠.٦%، يليه التابلت بنسبة ٣٠.١%، ثم الساعة الذكية بنسبة ٢٨.٣%، ثم أجهزة الألعاب الرقمية بنسبة ١٨.٤%، يليها الأجهزة القابلة للارتداء بنسبة ١٣.٢%، وفي النهاية جاء استخدام الحاسوب المكتبي، الذي يعد استخدامه نادراً للغاية، فلم يفد سوى نسبة ٤.٩% فقط من المبحوثين باستخدامه.

وتعد هذه النتيجة، التي تجعل الهاتف الذكي على قمة الأجهزة الأكثر اعتمادية لدى المستخدمين، متوائمة مع سمة العصر الرقمي الذي يتسم بالقابلية للتحريك والفورية، فقد أصبح من الضروري الاعتماد على أجهزة توفر المرونة والحرية في الحركة مع دوام التشبيك بالإنترنت، وضمان الاستمرارية في التواصل الاجتماعي مع الآخرين وإمكانية

الوصول للمحتوى من أي مكان، إضافة إلى إمكانية استخدامها لأغراض أخرى، مثل الترفيه والألعاب، واستخدامات أخرى احترافية مثل التصوير والمونتاج، مما يجعله جهازًا متكاملًا بصورة باهرة يستطيع أن يلبي احتياجات الفرد، سواء كانت احتياجات اجتماعية أو مهنية أو ترفيهية... إلخ، لذا كانت الهواتف الذكية أكثر الأجهزة التي يعتمد عليها المبحوثون.

وربما يدلل الاعتماد على الكمبيوتر المحمول (لابتوب) في مرتبة تالية للهواتف الذكية على الاحتياجات المهنية للمستخدم، مثل العمل والدراسة، ويمكن تفسير الاعتماد على التليفزيون الذكي بصورة معقولة بأهمية الترفيه لدى المبحوثين، فهو لم يعد مجرد شاشة تلفاز عادية، ولكن يُمكن من مشاهدة المنصات الرقمية المتخصصة مثل (شاهد – Watch it – Apple TV – Netflix ... وغيرها) عبر واجهته الكبيرة، أو تشبيكه بأجهزة الألعاب لمتعة لعب أكثر انغماسًا. وبينما تؤدي الأجهزة اللوحية (التابلت) المهام ذاتها التي يؤديها الهاتف الذكي، إلا أن كبر حجمه يمكن أن يمثل عائقًا أمام المرونة وقابلية الحركة مقارنة بالهاتف الذكي، ما يجعل اقتناءه إضافة ربما ترفيهية للمستخدم وليست أساسية مقارنة بالهاتف، وكذلك الأمر للساعات الذكية. أما أجهزة الألعاب الإلكترونية، فلن يسعى لاقتنائها إلا الأشخاص الأكثر اندماجًا في تجربة الألعاب؛ إذ يؤدي الهاتف أو جهاز الكمبيوتر المحمول هذه المزايا للاعب الذي يرغب في هذا الترفيه بإمكانات وأدوات متاحة، وهو ما جعلها في ترتيب متأخر. وتمثل الأجهزة القابلة للارتداء، مثل أساور اللياقة البدنية، مزايا يمكن للتطبيقات المدمجة بالهواتف الذكية أن تؤدي مهامها، لذلك لا يعتمد عيلها كثير من المبحوثين. ويمكن تفسير انخفاض الاعتماد على جهاز الكمبيوتر المكتبي بخصائصه التي لم تعد تناسب الجمهور، وهي عدم القابلية للحركة؛ إذ يتحتم على مستخدمه البقاء في مكان محدد لاستخدامه.

**جدول (٤) مستوى الاستخدامات الرقمية للمبحوثين**

| مستوى استخداماتك الرقمية | دائما | أحيانًا | نادرا | المتوسط | الانحراف المعياري | الوزن النسبى |
|---|---|---|---|---|---|---|
| شبكات التواصل الاجتماعي مثل: فيسبوك – تويتر - يوتيوب – انستجرام... إلخ | 355 | 30 | – | 2.92 | .268 | 97.3 |
| | 92.2% | 7.8% | – | | | |
| المواقع الإلكترونية | 176 | 175 | 34 | 2.37 | .641 | 79 |
| | 45.7% | 45.5% | 8.8% | | | |
| خدمات البريد الإلكتروني | 151 | 145 | 89 | 2.16 | .774 | 72 |
| | 39.2% | 37.7% | 23.1% | | | |
| محركات البحث مثل: جوجل كروم، فايرفوكس، إنترنت اكسبلورر،... إلخ | 230 | 144 | 11 | 2.57 | .551 | 85.7 |
| | 59.75 | 37.4% | 2.9% | | | |
| منصات مشاركة الملفات السحابية مثل: جوجل درايف Google Drive – دروب بوكس Dropbox- وغيرها | 152 | 166 | 67 | 2.22 | .722 | 74 |
| | 39.5% | 43.1% | 17.4% | | | |
| تطبيقات متابعة الصحة واللياقة البدنية | 43 | 182 | 160 | 1.70 | .660 | 56.7 |
| | 11.25 | 47.3% | 41.6% | | | |
| تطبيقات المراسلة والدردشة المختلفة مثل: واتس آب – ماسنجر - تليجرام – بوتيم – فايبر... إلخ | 343 | 42 | – | 2.89 | .312 | 96.3 |
| | 89.1% | 10.9% | – | | | |
| الألعاب الرقمية المتصلة بالإنترنت | 109 | 188 | 88 | 2.05 | .714 | 68.3 |
| | 28.3% | 48.8% | 22.9% | | | |
| الاستماع إلى الموسيقى عبر تطبيقات الموسيقى مثل تطبيقات Apple Music - Spotify - SoundCloud - YouTube Music | 150 | 131 | 104 | 2.12 | .804 | 70.7 |
| | 39% | 34% | 27% | | | |
| التسوق الإلكتروني عبر مواقع مثل: نون – جوميا – أمازون... وغيرها | 123 | 193 | 69 | 2.14 | .693 | 71.3 |
| | 31.9% | 50.15 | 17.9% | | | |

تشير نتائج الجدول السابق (٤) إلى مستوى الاستخدامات الرقمية للمبحوثين، وكان استخدام شبكات التواصل الاجتماعي مثل: فيسبوك ويوتيوب وانستجرام وتويتر وغيرها أكثر الاستخدمات المبحوثين عبر الإنترنت، فجاء في الترتيب الأول بوزن نسبي

97.3%، وجاء استخدام تطبيقات المراسلة والدردشة المختلفة مثل: واتس آب – ماسنجر - تليجرام – بوتيم – فايبر... إلخ في الترتيب الثاني بوزن نسبي 96.3%، يلي ذلك استخدام محركات البحث مثل: جوجل كروم، فايرفوكس، انترنت اكسبلورر،... إلخ بوزن نسبي 85.7%، ثم الاعتماد على المواقع الإلكترونية بمتوسط حسابي 2.37 ووزن نسبي 79%، يليه الاعتماد على منصات مشاركة الملفات السحابية مثل: جوجل درايف Drive Google – دروب بوكس Dropbox- وغيرها بوزن نسبي 74%، ثم الاعتماد على خدمات البريد الإلكتروني بوزن نسبي قدره 72%، يلي ذلك التسوق الإلكتروني عبر مواقع التسوق المختلفة مثل: نون وجوميا وأمازون... وغيرها بوزن نسبي 71.3%، يليه الاستماع إلى الموسيقى عبر تطبيقات الموسيقى مثل سبوتيفاي Spotify وايتيونز Apple Music وساوندكلاود SoundCloud وموسيقى يوتيوب YouTube Music بوزن نسبي قدره 70.7%، ثم الألعاب الرقمية المتصلة بالإنترنت بوزن نسبي 68.3%، يلي ذلك تطبيقات متابعة الصحة واللياقة البدنية بوزن نسبي 56.7%.

وتفسر الباحثة هذه النتيجة بزيادة استخدام التطبيقات التي تلبي حاجات الاتصال الاجتماعية للجمهور في المرتبة الأولى، التي يمثلها كل من **شبكات التواصل الاجتماعي وتطبيقات المراسلة**؛ إذ توفر وسيلة للبقاء على تواصل مع الأصدقاء والانفتاح على الآخر، ومشاركة الأفكار والمشاعر، والتفاعل مع الآخرين، إضافة إلى الاحتياجات المعرفية التي تلبيها، مثل التعرف على الأحداث والأخبار الجارية. وتفسر الباحثة تراجع الاعتماد على البريد الإلكتروني، مقابل زيادة الاعتماد على تطبيقات المراسلة الفورية، بزيادة أهمية حالة الفورية في الرد، ووجود حالة من نفاد الصبر لدى المستخدم الذي يفترض سرعة رد الآخرين عبر تطبيقات المراسلة عن البريد الإلكتروني؛ بينما أصبح اقتصار البريد الإلكتروني إلى حد كبير على المراسلات الرسمية، وعدّه أداة مساعدة لتسجيل حسابات رقمية على مختلف المواقع والتطبيقات، وإن كانت توجد طرق أخرى الآن، مثل التسجيل بحساب الشبكات الاجتماعية أو رقم الهاتف.

وتعد محركات البحث وسيلة أساسية اليوم في البحث عما أُشكل على المستخدم، فهي أداة للوصول السريع لأي معلومة، فباتت (google it) كلمة متداولة لمن يسأل عن معلومة، وتعني "استخدم محرك جوجل للبحث عما تسأل"، وتعكس هذه العبارة قناعة تقضي بأن أي تساؤل يمكن أن يدور في ذهن المستخدم من المتوقع أن يجد إجابته عبر محركات البحث، التي يُعدّ جوجل أشهرها. كما أن مشاركة الملفات بخدمات التخزين السحابية واستخدام البريد الإلكتروني تُمثل احتياجات أساسية للمستخدم، خاصة في العمل أو الدراسة، سواء بغرض التخزين الشخصي أو تيسير تشاركية الملفات، لذلك كان اعتماد نسبة كبيرة من المستخدمين عليها.

بينما جاءت بقية الاستخدامات الرقمية في ترتيب لاحق، حيث الاستخدامات التجارية المتمثلة في التسوق الإلكتروني التي تتوقف على قدر الثقة في الموقع أو التطبيق وسمعته الراسخة لدى الجمهور، التي تعزز إقبال الجمهور على الاعتماد عليه طريقة في التسوق، والاستخدامات الترفيهية المتمثلة في الاستماع إلى تطبيقات الموسيقى والألعاب الرقمية، إذ يُمكن عدّها أنشطة ترفيهية تعزز من حالة الاستمتاع لدى المستخدم، ثم تطبيقات الصحة واللياقة التي تعمل على تحفيز المستخدم على ممارسة التمارين ومراقبة صحته.

وينبئ مستوى هذه الاستخدامات إلى إدماج الرقمنة في جميع مناحي حياة الفرد اليومية، فاستخدام الأجهزة الرقمية وتطبيقات الإنترنت المختلفة بات أمراً لا مناص منه، ما نتج عنه أن أصبح الفرد أسيراً لهذه التسهيلات، ومولعا بكيفية تطويعها في حياته، مما يعني بالتبعية اتساع بصمته الرقمية، حيث زيادة البيانات التي يتركها المستخدم خلفه وتتلقاها شركات التكنولوجيا والاتصالات، وتسجيل بيانات المستخدمين، مثل البيانات الشخصية عند التسجيل في هذه الخدمات أو عند الإفصاح عنها في أي مرحلة من الاستخدام، أو بيانات التصفح والنقر على الروابط، وزيارته للمواقع والتطبيقات، وبيانات حول تفاعله، والوسائط المتعددة التي يشاهدها أو يُحمِّلها وبيانات موقعه الجغرافي... وغير ذلك من تفاعلات في البيئة الرقمية.

وتتفق هذه النتيجة مع نتائج دراسة (سحر أحمد غريب، ٢٠٢١)[81]، التي أشارت إلى ارتفاع معدل تعرض الجمهور لفيسبوك بشكل كبير، يلي ذلك استخدام تطبيق واتس آب للمراسلة.

**جدول (٥) الجهات التى يعتقد المبحوث أن بإمكانها الاطلاع على بياناته وتجميعها**

| من تعتقد أن بإمكانه الاطلاع على بياناتك وأنشطتك على الإنترنت ويمكنه جمعها؟ | ك | % |
|---|---|---|
| منصات الشبكات الاجتماعية، مثل Facebook، LinkedIn، Twitter، Instagram، YouTube | 228 | 59.2% |
| تطبيقات الهاتف المحمول التي أستخدمها | 213 | 55.3% |
| مواقع الويب التي أزورها | 194 | 50.4% |
| الشركات والمواقع التي أشتري منها | 187 | 48.6% |
| محركات البحث | 180 | 46.8% |
| الحكومات | 161 | 41.8% |
| مزود خدمة الإنترنت الخاص بي | 160 | 41.6% |
| قراصنة الإنترنت | 155 | 40.3% |
| جهات الاتصال التي لدي على الهاتف | 136 | 35.3% |
| يمكن لأي شخص العثور على معلومات عني من خلال بحث بسيط، مثل الأصدقاء وأصحاب العمل المحتملين | 89 | 23.1% |

تشير بيانات الجدول السابق (٥) إلى الجهات التي يعتقد المستخدم أن بإمكانها الاطلاع على أنشطته الرقمية المختلفة وبياناته وتجميعها، ويأتي على رأسها منصات الشبكات الاجتماعية مثل Facebook، LinkedIn، Twitter، Instagram، YouTube؛ إذ يعتقد ٥٩.٢% أنها تقدر على ذلك، يلي ذلك تطبيقات الهاتف المحمول التي يستخدمها بنسبة ٥٥.٣%، ثم مواقع الويب التي يزورها بنسبة ٥٠.٤%، ثم الشركات والمواقع التي يشتري منها بنسبة ٤٨.٦%، ثم محركات البحث بنسبة ٤٦.٨%، يليها الحكومات بنسبة ٤١.٨%، ثم مزود خدمة الإنترنت التي يستخدمها المستخدم

بنسبة ٤١.٦%، ثم قراصنة الإنترنت بنسبة ٤٠.٣%، ثم جهات الاتصال بنسبة ٣٥.٣%، ثم اعتقاده أنه بإمكان أي شخص العثور على معلومات عنه من خلال بحث بسيط، مثل الأصدقاء وأصحاب العمل المحتملين، وذلك بنسبة ٢٣.١% من المبحوثين.

ويمكن تفسير هذه النتيجة نظراً لكون الشبكات الاجتماعية هي الأكثر استخداماً؛ إذ ينغمس فيها المبحوثون وفقًا لبيانات الجدول (٤)، وكونها قائمة على مفهوم المشاركة الدائم، ونظراً لما قد يعاينه المستخدم من ارتباط بعض المحتوى الذي يظهر له، مثل التوجيه الإعلاني، واقتراح الأصدقاء، لنتائج شديدة الصلة به دون أن يبادر هو بالبحث عنها؛ فيترسخ لديه اعتقاد حول إمكانية هذه الشبكات في معرفة تفضيلات المستخدم واهتماماته وتحليلها وتقديم ما يُعتقد أنه مهم بالنسبة إليه، وكذلك الأمر في التطبيقات التي يتفاعل المستخدم معها منذ بداية عملية التسجيل وتقديمه معلومات مرجعية، وربما استجابته لاستطلاع لتحليل اهتماماته لعرض ما يناسبه في التطبيق، لا سيما في تطبيقات الصحة والرشاقة، ثم يتفاعل عبر إدخال مستحدثات حالته. وجاء في إثر ذلك مواقع الويب ومواقع التسوق الإلكتروني نظراً لكونهما جهات تطلع على قدر كبير من البيانات مثل تفضيلات المستخدم وعناصر البحث التي يقوم بها وما إلى ذلك. وتتفق هذه النتيجة مع دراسة (Michael, M., and D. Lupton, 2017)[82]، التي أشارت إلى اعتقاد المبحوثين أن كلًا من جوجل وفيسبوك تتبع تفضيلاتهم وعاداتهم.

ويمكن تفسير رؤية المبحوثين أن كلًا من قدرة جهات الاتصال، أو إمكانية أي شخص من العثور على معلومات عنه من خلال البحث عنه؛ دليل على رؤية المستخدمين للإمكانات المحدودة لهذه الجهات للوصول إلى بياناته، لأن هؤلاء المستخدمين العاديين ليس بإمكانهم الوصول إلى بيانات المستخدم إلا بالقدر الذي يفصح هو عنه، أي أن اعتقاد المستخدم بالجهات التي يمكن أن تصل بياناته وتجمعها رهن بقدرة هذه الجهات على سبر ما يخفيه في غرفة مظلمة بعيداً عما يظهره، وهو ما يعني وصولها إلى البصمة السلبية غير النشطة، أما ما ينشره هو بنفسه، ويتمثل في البصمة الإيجابية، فهو وحده الذي يمكن لجهات الاتصال والأصدقاء لديه معرفته.

ولما كان جمع البيانات عن المستخدم راسخًا وفق هذا الاعتقاد، بات من المحتم التعرف على مستوى حساسية البيانات المختلفة لدى المستخدمين، وهو ما يشير إليه الجدول الآتي:

**جدول (٦) حساسية بعض أنواع المعلومات بالنسبة للمستخدم**

| ما مدى حساسية المعلومات التالية بالنسبة لك؟ | حساسة للغاية | إلى حد ما | غير حساسة | المتوسط Mean | الإنحراف المعياري Std. | الوزن النسبى |
|---|---|---|---|---|---|---|
| المعلومات الشخصية الأساسية، مثل: الاسم وتاريخ الميلاد والنوع ورقم الهاتف والعنوان الحالي والبريد الإلكتروني والصورة الشخصية | 105 | 226 | 54 | 2.13 | .630 | 71 |
| | 27.3% | 58.7% | 14% | | | |
| المعلومات الشخصية الحساسة، مثل: الحالة الصحية أو التوجهات السياسية أو المعتقدات الدينية | 104 | 51.4% | 83 | 2.05 | .696 | 68.3 |
| | 17% | 51.4% | 21.6% | | | |
| معلومات الشراء عبر الإنترنت | 155 | 122 | 108 | 2.12 | .819 | 70.7 |
| | 40.3% | 31.7% | 28.1% | | | |
| بيانات نشاطك في الويب وفي التطبيقات (مثل المواقع التي تزورها والتطبيقات التي تستخدمها) | 100 | 146 | 139 | 1.90 | .782 | 63.3 |
| | 26% | 37.9% | 36.1% | | | |
| عنوانIP الخاص بالجهاز الذي تستخدمه ويمكنه تحديد موقعك | 101 | 203 | 81 | 2.05 | .666 | 68.3 |
| | 26.2 | 52.7% | 21% | | | |
| نشاط البريد الإلكتروني ويشمل الرسائل التي ترسلها وتستقبلها والمرفقات التي بها وعناوين بريد الآخرين | 220 | 121 | 44 | 2.46 | .691 | 82 |
| | 57.1% | 31.4% | 11.4% | | | |
| المعلومات المالية مثل رقم الحساب البنكي | 289 | 46 | 50 | 2.62 | .705 | 87.3 |
| | 75.1% | 11.9% | 13% | | | |
| سجل المواقع الجغرافية (الأماكن التي تذهب إليها وسفرياتك) | 93 | 199 | 93 | 2.00 | .696 | 66.7 |
| | 24.2% | 51.7% | 24.2% | | | |

| ما مدى حساسية المعلومات التالية بالنسبة لك؟ | حساسة للغاية | إلى حد ما | غير حساسة | المتوسط Mean | الإنحراف المعياري Std. | الوزن النسبى |
|---|---|---|---|---|---|---|
| جهات الاتصال الخاصة بك | 188 | 158 | 39 | 2.39 | .664 | 79.7 |
| | 48.8% | 41% | 10.1% | | | |
| الصور الشخصية ومقاطع الفيديو الخاصة بك | 276 | 67 | 42 | 2.61 | .677 | 87 |
| | 71.7% | 17.4% | 10.9% | | | |
| نوع المتصفح والجهاز الذي تستخدمه | 68 | 184 | 133 | 1.83 | .703 | 61 |
| | 17.7% | 47.8% | 34.5% | | | |
| سجل المشاهدة والبحث على يوتيوب | 108 | 156 | 121 | 1.97 | .771 | 65.7 |
| | 28.1% | 40.5% | 31.4% | | | |
| عمليات البحث التي تجريها عبر محركات البحث | 207 | 149 | 29 | 2.46 | .633 | 82 |
| | 53.8% | 38.7% | 7.5% | | | |

وفقًا لاتجاه الرأي لمقياس ليكرت الثلاثي (دائمًا: من 2.34 إلى 3)، (أحيانًا: من 1.67 إلى 2.33)، (نادرًا: من 1 إلى 1.66) وباستقراء نتائج الجدول السابق (٦) عن مقدار حساسية بعض المعلومات التي يحتمل معرفتها عن المستخدم عبر أنشطته على الإنترنت؛ يأتي في مقدمتها المعلومات المالية، مثل رقم الحساب البنكي، التي تُعدّ حساسة للغاية بوزن نسبي 87.3%، يليها الصور الشخصية ومقاطع الفيديو الخاصة بالمستخدم، وقُدِّرت بأنها حساسة للغاية بوزن نسبي 87%، ثم أشار المبحوثون إلى أن نشاط البريد الإلكتروني ويشمل الرسائل التي يرسلها ويستقبلها والمرفقات التي بها وعناوين بريد الآخرين حساسة للغاية أيضًا وذلك بوزن نسبي 82%، وعمليات البحث التي يجريها عبر محركات البحث بوزن نسبي 82%، ثم جهات الاتصال الخاصة به بوزن نسبي 79.7%، ثم المعلومات الشخصية الأساسية، مثل: الاسم وتاريخ الميلاد والنوع ورقم الهاتف والعنوان الحالي والبريد الإلكتروني والصورة الشخصية بوزن نسبي 71%، ثم معلومات الشراء عبر الإنترنت بوزن نسبي 70.7%، يلي ذلك عنوان IP الخاص بالجهاز الذي يستخدمه ويمكنه تحديد موقع المستخدم بوزن نسبي 68.3%، ثم المعلومات الشخصية الحساسة، مثل: الحالة الصحية أو التوجهات السياسية أو المعتقدات الدينية بوزن نسبي 68.3%، ثم سجل المواقع الجغرافية (الأماكن التي تذهب

إليها وسفرياتك) بوزن نسبي 66.%، ثم سجل المشاهدة والبحث على يوتيوب بوزن نسبي 65.%، يلي ذلك بيانات نشاط الويب والتطبيقات (مثل المواقع التي يزورها والتطبيقات التي يستخدمها) بوزن نسبي 63.3%، وفي الترتيب الأخير نوع المتصفح والجهاز الذي يستخدمه بوزن نسبي 61%.

ومن خلال هذه النتائج يمكن القول أنه على الرغم من أن التسوق الإلكتروني لم يكن على رأس الاستخدامات الرقمية للمبحوثين، فقد سبقه استخدام الشبكات الاجتماعية وتطبيقات المراسلة ومحركات البحث والخدمات السحابية والبريد الإلكتروني وفقًا لنتائج الجدول (٤)، فإن نتائج هذا الجدول التي تشير إلى أن المعلومات المالية والحسابات المصرفية أكثر المعلومات حساسية بالنسبة للمبحوثين يمكن أن يُفسّره بحجم المخاطر التي يعتقد المستخدم أنها قد تؤدي إلى خسائر كبيرة بالنسبة إليه، لا سيما إذا كانت خسائر مالية كبيرة إذا لم تكن بياناته المصرفية بأمان.

أما الصور الشخصية والفيديو الخاص بالمستخدم، بوصفها جزءاً من هوية الذات والبصمة الرقمية للمستخدم، فقد جاءت أيضًا في مرتبة متقدمة نظراً لأن تأثير الصور والفيديو الرقمي قد يكون أقوى من تأثير الكلمات والمعلومات الشخصية الأخرى، فالصورة بما تحمله من دلالات ومشاعر وتجارب خاصة للفرد يمكن أن تمس مكانته إذا استُغلت بطريقة خاطئة، أو أن نفسه تهتز من التعليقات التي ربما تطاله، لذا فهي تعد ذات حساسية كبيرة حتى أكثر من معلومات كاسمه أو عنوانه، وقد زخرت مواقع التواصل الاجتماعي بمقاطع فيديو عفوية لأشخاص اقتُطعت صورة منها ووُسمت بهاشتاجات واستخدمت في سياقات مختلفة، مما قد يؤثر في حالة الأفراد وصورة الذات لديهم.

ويأتي نشاط البريد الإلكتروني، ويشمل عنوان البريد الإلكتروني نفسه والرسائل التي يرسلها المستخدم ويستقبلها، والمرفقات التي بها وعناوين بريد الآخرين، في مرتبة متقدمة من المعلومات الحساسة للغاية من وجهة نظر المستخدم؛ إذ يمكن أن يحتوي على معلومات سرية، مثل المراسلات الشخصية الخاصة، أو مراسلات سرية خاصة بالعمل، لذا كان من الأهمية أن تبقى هذه المعلومات غير متاحة للعامة، ويفترض أن تبقى سرية، لذلك يمكن عدّ البريد الإلكتروني للمستخدم بيانات خاصة جداً لا ينبغي تداولها مع

جهات خارجية وعدم إدراجه في قوائم بريدية دون علمه، مما قد يجعله عرضة للفيروسات أو الاحتيال أو حتى ازدحام البريد برسائل غير مرغوب فيها. ورغم أن عمليات البحث التي يجريها المستخدم عبر محركات البحث قد لا تكون حساسة، فإن المبحوثين يعتقدون أنها تمثل قدراً من الحساسية، فقد يرغب بعضهم في الاحتفاظ بخصوصية بعض عمليات البحث، وكذلك سجل المشاهدة والبحث على يوتيوب، وبيانات نشاط المواقع التي يزورها والتطبيقات التي يستخدمها.

ونظراً لأهمية حماية بيانات جهات الاتصال لدى المستخدم، فقد عدَّها أغلب المبحوثين ضمن فئة المعلومات الحساسة للغاية حتى يتوقع هؤلاء الأشخاص الحفاظ على سرية بياناتهم، ويمكن أن تضم بيانات جهات الاتصال أرقام الهواتف وعناوين البريد الإلكتروني لهم، ومعرفات حساباتهم على مواقع التواصل الاجتماعي؛ إذ يمكن إساءة استخدامها عبر الرسائل الاحتيالية من جهات الاتصال الموثوقة لأغراض الاستدراج والابتزاز والسرقة، فضلًا عن التسويق المستهدف أيضاً.

وعدَّ المبحوثون المعلومات الشخصية، مثل الاسم وتاريخ الميلاد والنوع ورقم الهاتف والعنوان والبريد الإلكتروني والصورة الشخصية، ومعلومات أخرى كالحالة الصحية أو التوجهات السياسية أو المعتقدات الدينية، أقل حساسية من المعلومات السابقة، وتعتقد الباحثة أن درجة حساسية مثل هذه المعلومات للأفراد قد تختلف وفقًا لطبيعة استخدامها بصفتها هوية الفرد وجزءاً من شخصيته الواقعية، فبينما يمكن عدّ الاسم من المعلومات الأقل حساسية؛ فقد لا يحبذ أن يعرف الآخرين محل إقامته أو صورته الشخصية، أو يطلع الآخرون على توجهاته، لذا تكون أكثر حساسية بالنسبة إليه. وعادة لا تُعدّ معلومات التسوق عبر الإنترنت، مثل طبيعة السلعة ومواصفاتها، حساسة كمعلومات الفرد الشخصية، إلا إذا ارتبطت بالمعلومات المالية، ومع ذلك لا يمكن تجاهل كونها حساسة إلى حد ما، فمن خلالها يمكن تحديد اهتمامات الأفراد.

وقد يُعدّ عنوان IP بمثابة البصمة السلبية غير النشطة ضمن المعلومات ذات الحساسية لدى المستخدمين لعدة أسباب، قد يكون منها الاحتياج إلى إخفاء عنوان IP من أجل المساعدة في تجاوز الإقصاء الجغرافي للوصول لمواقع محجوبة في منطقة

جغرافية معينة. بينما قد تُعدّ مشاركة المبحوثين أماكن زاروها أو سافروا إليها نوعًا من المشاركة الاجتماعية المحببة، ويعد ضمن ما يشكل البصمة الرقمية الإيجابية أو النشطة، لذا لم تكن معلومات حساسة بصورة كبيرة. وبينما تجمع شركات التكنولوجيا والاتصالات معلومات متعلقة بالأجهزة، مثل نوع الجهاز، وإصدار التشغيل، والمعرفات الفريدة، ومعلومات عن شبكة الاتصال، بما في ذلك رقم الهاتف، فعلى سبيل المثال، تقرن جوجل هذه البيانات بحسابات المستخدمين لديها، لذا يمكن تفسير تصنيف المستخدمين نوع المتصفح والجهاز معلومات غير حساسة بصورة كبيرة لعدم المعرفة الكافية لما يمكن أن تعنيه هذه المعلومات كأداة لتحديد الهوية الشخصية.

وتتفق هذه النتائج مع نتائج دراسة (Marinelli, A., & Parisi, S. 2022)[83]، التي أشارت إلى حساسية المعلومات المصرفية، كما أشارت إلى حساسية المعلومات الشخصية المتعلقة بالهوية الحقيقية والبيانات الشخصية، كما تتفق مع نتائج دراسة ( Metzger, M. J. 2007)[84]، التي وجدت أنه في سياق التجارة الإلكترونية يكون الأفراد أكثر وعيًا بالمخاطر عند وجود معاملات مالية. وتتفق النتائج مع دراسة (محمود محمد، ٢٠٢٢)[85]، التي أشارت إلى أن المستخدم لا يشارك بيانات مثل بيانات البطاقات البنكية بسهولة عبر تطبيقات التسويق الإلكتروني، وكانت أبرز أنواع البيانات التي يكشفها المستخدم طواعية هي النوع والاسم والعمر والتخصص الدراسي. كما تتفق أيضًا مع نتائج دراسة (مها عبد الحميد، ٢٠٢٢)[86]، التي أشارت إلى إدخال المبحوثين بياناتهم الشخصية على التطبيقات التسويقية.

**جدول (٧) اعتقاد المستخدم للمدة الزمنية المقبولة لاحتفاظ الشركات أو المؤسسات ببياناته المختلفة**

| ما المدة الزمنية التى تعتقد أنه ينبغى على الشركات أو المؤسسات التالية الاحتفاظ ببياناتك | المدة التى هم في حاجة إلى ذلك | مدة زمنية بسيطة (أسابيع أو شهور قليلة) | أثناء الاستخدام فقط | لا ينبغى لهم حفظ أي معلومات | المتوسط | الانحراف المعياري | الوزن النسبى |
|---|---|---|---|---|---|---|---|
| محرك البحث الذي تستخدمه | 116 | 121 | 95 | 53 | 2.22 | 1.026 | 55.5 |
| | 30.1% | 31.4% | 24.7% | 13.8% | | | |
| مزود خدمة البريد الإلكتروني الخاص بك | 101 | 110 | 102 | 72 | 2.38 | 1.066 | 59.5 |
| | 26.2% | 28.6% | 26.5% | 18.7% | | | |
| مواقع التواصل الاجتماعي | 60 | 147 | 105 | 73 | 2.50 | .971 | 62.5 |
| | 15.6% | 38.2% | 27.35 | 19% | | | |
| المعلنون الذين يضعون إعلانات على المواقع التي تزورها | 93 | 79 | 135 | 78 | 2.51 | 1.068 | 62.8 |
| | 24.25 | 20.5% | 35.1% | 20.3% | | | |
| التطبيقات التي تستخدمها | 66 | 126 | 121 | 72 | 2.48 | .984 | 62 |
| | 17.1% | 32.7% | 31.4% | 18.7% | | | |
| الجهات التي تشتري منها عبر الإنترنت | 67 | 134 | 80 | 104 | 2.43 | 1.066 | 60.8 |
| | 17.45 | 34.8% | 20.8% | 27% | | | |
| المواقع والمدونات والمنتديات التي تزورها | 57 | 120 | 100 | 108 | 2.33 | 1.039 | 58.3 |
| | 14.8% | 31.25% | 26% | 28.1% | | | |

تشير نتائج هذا الجدول (٧) إلى الزمن الذي يعتقده المستخدم حول مدة بقاء بياناته لدى جهات وشركات التكنولوجيا والاتصال التي يمكن أن تمثل إشكالية لاستدامة بصمته الرقمية إذا بقيت لفترة طويلة، بحيث تعكس هذه المدة الزمنية وفقًا لمقياس ليكرت الرباعي درجة الشدة نحو خوف المستخدم على بصمته الرقمية، فيدل رفضه احتفاظ الجهات لبياناته على خوف شديد على بصمته الرقمية (من ٣.٢٥ إلى ٤)، وعلى الجهة العكسية بالمقياس يشار إلى الموافقة على احتفاظها ببياناته لمدة زمنية غير معلومة ولا نهائية إلى عدم الخوف على بصمته الرقمية (من ١ إلى ١.٧٤)، بينما يعد رضاه عن احتفاظها بالبيانات لمدة زمنية بسيطة يمكن أن تمتد إلى أسابيع أو أشهر قليلة إلى خوف بسيط (من ١.٧٥ إلى ٢.٤٩)، ويدلل اتجاهه حول إمكانية الاحتفاظ بياناته أثناء استخدامه فقط بحيث ينتهي تملك الجهات للبيانات بمجرد انتهاء الجلسة إلى خوف

متوسط على بصمته الرقمية (من ٢.٥٠ إلى ٣.٢٤). وتشير النتائج إلى أن اعتقاد المستخدمين للمدة الزمنية التي ينبغي على المعلنين الذين يضعون إعلانات على المواقع التي يزورونها ومواقع التواصل الاجتماعي إلى أعلى وزن نسبي قيمته ٦٢.٨%، يليها مواقع التواصل الاجتماعي بوزن نسبي ٦٢.٥%، ثم التطبيقات التي يستخدمها بوزن نسبي ٦٢%، ثم الجهات التي يشتري منها عبر الإنترنت بوزن نسبي ٦٠.٨%، ثم مزود خدمة البريد الإلكتروني الخاص به بوزن نسبي ٥٩.٥%، ثم المواقع والمدونات والمنتديات التي يزورها بوزن نسبي ٥٨.٣%، وأخيراً محركات البحث بوزن نسبي ٥٥.٥%.

وباستقراء هذه البيانات، لم تظهر استجابات المبحوثين خوفًا شديدًا على بصمتهم الرقمية، حيث لم يلاحظ وجود اتجاه قوي نحو خيارات عدم السماح بحفظ البيانات لدى أي من الجهات المختلفة، ويمكن تفسير ذلك كنتيجة للتسليم بحتمية جمع البيانات، بينما أظهرت جميع اتجاهات المستخدمين خوفًا متوسطًا على بصمتهم الرقمية، وذلك للجهات التالية: المعلنين الذين يضعون إعلانات على مواقع الويب التي يزورونها، ومواقع التواصل الاجتماعي، بينما كانت المتوسطات الإجمالية الدالة على خوف بسيط للجهات: التطبيقات التي يستخدمها، والجهات التي يشتري منها عبر الإنترنت، ومزود خدمة البريد الإلكتروني الخاص به، والمواقع والمدونات والمنتديات، ومحرك البحث الذي يستخدمه. إلا أن الاتجاه السائد لدى أفراد العينة في كل من الجهات الثلاث الأخيرة – وفقًا للمنوال الخاص بكل جهة– هو الاحتفاظ ببياناتهم لفترة زمنية بسيطة، ربما تصل لبضعة أسابيع أو أشهر.

ويمكن أن يعد حذف الجهات لبيانات المستخدم بعد الاحتفاظ بها لفترات محددة ومعقولة أن يشعر المستخدم بمزيد من الأمان، فقد يكون مثيراً للحيرة أن يجد الفرد بياناته، مثل سجل تصفحه ونقراته على الروابط أن تبقى مخزنة لسنوات طويلة، إضافة إلى أهمية الشفافية، ليس فقط في الإعلان عن البيانات التي تُجمع، ولكن مدة الاحتفاظ بها.

**جدول (٨) الوعي بمفهوم البصمة الرقمية**

| الوعي بالبصمة الرقمية | موافق | محايد | غير موافق | المتوسط | الإنحراف المعيارى | الوزن النسبى |
|---|---|---|---|---|---|---|
| أدرك أن المعلومات المتعلقة بي في البيئة الرقمية يمكنها الظهور مستقبلًا في حياتي الدراسية أو المهنية أو الخاصة | 144 | 183 | 58 | 2.22 | .690 | 74 |
| | 37.4% | 47.5% | 15.1% | | | |
| لا يستطيع أحد أن يمتلك بياناتي دون إذني | 64 | 54 | 267 | 1.47 | .764 | 49 |
| | 16.6% | 14% | 69.4% | | | |
| أعلم أن أيا من المعاملات التي أقوم بها في البيئات الرقمية لن تكون مجهولة المصدر ولن تكون سرية | 235 | 114 | 36 | 2.52 | .662 | 84 |
| | 61% | 29.6% | 9.4% | | | |
| أفكر جيدًا عند استخدامي للبيئة الرقمية لأني أعرف بوجود من يجمع بياناتي دون أن أفصح عنها | 206 | 129 | 50 | 2.41 | .709 | 80.3 |
| | 53.5% | 33.5% | 13% | | | |
| يمكن لشركات التكنولوجيا والاتصالات والمواقع التي أستخدمها تحديد مكاني دون أن أذكره | 217 | 61 | 107 | 2.29 | .873 | 76.3 |
| | 56.4% | 15.8% | 27.8% | | | |
| يمكن التحقق من سمعة الآخرين من خلال البحث عنهم عبر الإنترنت | 245 | 110 | 30 | 2.56 | .635 | 85.3 |
| | 63.6% | 28.6% | 7.8% | | | |
| أعتقد أن شركات التكنولوجيا والاتصالات التي أستخدم منصاتها الرقمية تجمع بيانات لا أتوقعها | 226 | 127 | 33 | 2.50 | .650 | 83.3 |
| | 58.7% | 32.7% | 8.6% | | | |
| أعلم أن كل ما أفعله في البيئة الرقمية سيكون مخزنًا ومعلومًا لدى آخرين | 192 | 153 | 40 | 2.39 | .669 | 79.7 |
| | 49.9% | 39.7% | 10.4% | | | |
| أنا على دراية بمصطلح البصمة الرقمية | 158 | 169 | 58 | 2.26 | .703 | 75.3 |
| | 41% | 43.9% | 15.1% | | | |
| أعتقد أنه بالإمكان تتبع أنشطتي على الإنترنت بطرق لا أتوقعها | 128 | 148 | 109 | 2.05 | .784 | 68.3 |
| | 33.2% | 38.4% | 28.3% | | | |

وفقًا للجدول السابق (٨)، الذي يوضح الوعي بمفهوم البصمة الرقمية، يتضح أن أكثر ما يدركه المبحوثون هو إمكانية التحقق من سمعة الآخرين من خلال البحث عنهم

عبر الإنترنت بوزن نسبي ٨٥.٣%، يلي ذلك معرفته بأن أيًا من المعاملات التي يقوم بها في البيئات الرقمية لن تكون مجهولة المصدر ولن تكون سرية بوزن نسبي ٨٤%، ثم اعتقاده أن شركات التكنولوجيا والاتصالات التي يستخدم منصاتها الرقمية تجمع بياناته بطريقة ربما لا يتوقعها بوزن نسبي ٨٣.٣%، ثم التفكير الجيد عند استخدام البيئة الرقمية لمعرفته بوجود من يجمع بياناته دون أن يفصح عنها بوزن نسبي ٨٠.٣%، يلي ذلك معرفته أن كل ما يفعله في البيئة الرقمية سيكون مُخزَّنًا ومعلومًا لدى آخرين بوزن نسبي قدره ٧٩.٧%، ثم إدراكه أنه يمكن لشركات التكنولوجيا والاتصالات والمواقع التي يستخدمها تحديد مكانه دون أن يذكره بوزن نسبي ٧٦.٣%، يلي ذلك معرفته بمصطلح البصمة الرقمية بوزن نسبي ٧٥.٣%، ثم إدراكه أن المعلومات المتعلقة به في البيئة الرقمية يمكنها الظهور مستقبلًا في حياته الدراسية أو المهنية أو الخاصة بوزن نسبي ٧٤%، ثم اعتقاده أنه بالإمكان تتبع أنشطته على الإنترنت بطرق لا يتوقعها بوزن نسبي ٦٨.٣%، ثم اعتقاده أن لا أحد يستطيع أن يمتلك بياناته دون إذنه بوزن نسبي ٤٩%.

ويمكن إرجاع هذه النتائج إلى إدراك المبحوثين أن ما يشاركه المستخدم بنفسه أو ما يشاركه الآخرون عنه أو مراجعات الآخرين وتقييماتهم تجاه مقدمي الخدمات والأعمال لمن يعمل في سياق مهني أو تجاري، يمكن أن ينعكس على تكوين السمعة الرقمية له، التي تُعدّ امتدادًا لسمعته في الواقع، لذلك كانت استجابة المبحوثين الأعلى تجاه إمكانية التحقق من سمعة الآخرين، ونتيجة لهذا الإدراك، ورغم ما يتمتع به عالم الإنترنت من سيادة خاصية المجهولية، فإن هذه الخاصية يمكن أن تكون صحيحة فيما يخص البصمة النشطة؛ إذ يمكن للمستخدم التخفي تحت غطاء هوية زائفة لفعل ما يريد، إلا أن جميع هذه التصرفات والأفعال بالتأكيد لا تتمتع بالسرية والمجهولية التي يظنها الفرد لدى شركات وجهات تكنولوجيا الاتصالات، ويمكن أن تعد حالات تقفي أثر الجرائم الإلكترونية دليلًا على ذلك. ولدى المبحوثين اعتقاد كبير أن شركات التكنولوجيا والاتصالات التي يستخدمون منصاتها الرقمية تجمع بيانات ربما بطرق لا يتوقعونها، مما يدلل على وعي الجمهور بقدرات هذه الشركات التقنية، وهو ما يظهر أيضًا في وجود أقل استجابات للمبحوثين في المقياس اعتقادهم عدم قدرة أحد أن يمتلك بياناتهم دون إذنهم.

**جدول (٩) مستويات الوعى بمفهوم البصمة الرقمية**

| مستويات الوعى بالبصمة الرقمية | ك | % |
|---|---|---|
| منخفض | 5 | 1.3 |
| متوسط | 214 | 55.6 |
| مرتفع | 166 | 43.1 |
| الإجمالي | 385 | 100 |

تشير نتائج الجدول السابق (٩) إلى مستوى وعي الجمهور بالبصمة الرقمية، وقُدِّرت الإجابات وفقًا لمقياس ليكرت الثلاثي: موافق=3، محايد=2، غير موافق=1، ومن ثمَّ، فإن محصلة المقياس تتكون من (٢١) درجة، من (١٠: ٣٠)، مقسمة على ثلاثة مستويات: المستوى المنخفض (١٠- ١٦)، المستوى المتوسط (١٧-٢٣)، المستوى المرتفع (٢٤-٣٠). لذلك تشير هذه النتائج إلى وعي متوسط لدى أفراد العينة بالبصمة الرقمية، فقد كانت نسبة مستوى الوعي ٥٥.٦%، يلي ذلك وعي مرتفع لدى المبحوثين بنسبة ٤٣.١%، ونسبة قليلة جدًا من أفراد العينة كان لديهم وعي منخفض بنسبة ١.٣%.

وبمقارنة هذه النتيجة مع نتائج الدراسات المتعلقة بالخصوصية الرقمية، فإن النتائج تتفق مع ما جاءت به دراسة (سحر أحمد غريب، ٢٠٢١)[87]، فقد كان وعي الجمهور تجاه الخصوصية بدرجة متوسطة ثم مرتفعة. كما تتفق مع نتائج دراسة (سالي سعد، ٢٠٢١)[88]، التي أشارت إلى ارتفاع إدراك الجمهور لمفهوم الخصوصية الرقمية.

**جدول (١٠) مستويات المعرفة بالأنشطة الرقمية المكونة للبصمة الرقمية**

| الأنشطة التى يعتقد أنها تعمل على إتاحة المعلومات عنه وعن أنشطته عبر الإنترنت (الأنشطة التى تساعد في تكوين بصمتك الرقمية) | موافق | محايد | غير موافق | المتوسط | الإنحراف المعياري | الوزن النسبى |
|---|---|---|---|---|---|---|
| كتابة منشور، أو مشاركة صورة، أو التعليق على منشور شخص آخر، أو الإعجاب بصفحة، أو متابعة صفحة أو شخص بمواقع التواصل الاجتماعى | 256 | 84 | 45 | 2.55 | 0.695 | 85 |
| | 66.5% | 21.8% | 11.7% | | | |
| الصور ومقاطع الفيديو التي تنشرها بنفسك أو تحفظها عبر الإنترنت | 240 | 114 | 31 | 2.54 | 0.641 | 84.7 |
| | 62.35 | 29.6% | 8.1% | | | |
| رسائل البريد الإلكتروني التي ترسلها وتستقبلها | 196 | 102 | 87 | 2.28 | 0.810 | 76 |
| | 50.9% | 26.5% | 22.6% | | | |
| تفاعلاتك في المنتديات والمدونات والمجتمعات عبر الإنترنت | 225 | 148 | 12 | 2.55 | 0.557 | 85 |
| | 58.45 | 38.4% | 3.1% | | | |
| ملء نموذج تسجيل حساب جديد (سواء بموقع أو تطبيق أو شبكات التواصل الاجتماعى) | 208 | 115 | 62 | 2.38 | 0.748 | 79.3 |
| | 54% | 29.9% | 16.1% | | | |
| زيارة مواقع الويب وجلسات التصفح بها | 243 | 92 | 50 | 2.50 | 0.715 | 83.3 |
| | 63.15 | 23.9% | 13% | | | |
| تفاعلاتك في التطبيقات أو المتصفحات | 224 | 116 | 45 | 2.46 | 0.696 | 82 |
| | 58.25 | 30.15 | 11.7% | | | |
| عملية الشراء التي تجريها عبر الإنترنت (العنصر الذي تم شراؤه، ومن أين تم الشراء، ومتى، وتكلفته، وطريقة الدفع) | 273 | 60 | 52 | 2.57 | 0.718 | 85.7 |
| | 70.9% | 15.6% | 13.5% | | | |
| بيانات الحساب البنكي وبطاقة الائتمان التي وضعتها لأغراض مثل التسوق الإلكتروني أو المدفوعات الإلكترونية | 204 | 93 | 88 | 2.30 | 0.818 | 76.7 |
| | 53% | 24.2% | 22.9% | | | |
| إعطاء الأذونات للتطبيقات للوصول لمعلومات (مثل قائمة جهات الاتصال – موقعك الجغرافي...) | 241 | 99 | 45 | 2.51 | 0.696 | 83.7 |
| | 62.6% | 25.7% | 11.7% | | | |
| عنوانIP الخاص بك لتتبع نشاطك وجمع معلومات عن مكانك | 250 | 60 | 75 | 2.45 | 0.800 | 81.7 |
| | 64.9% | 15.6% | 19.5% | | | |
| يمكن لنظام تحديد المواقع العالمي (GPS) وإشارات شبكة WIFI جمع بيانات الموقع | 241 | 119 | 25 | 2.56 | 0.614 | 85.3 |
| | 62.6% | 30.9% | 6.5% | | | |
| البيانات البيومترية، مثل بصمات الأصابع والتعرف على الوجه ومسح قزحية العين | 195 | 124 | 66 | 2.34 | 0.753 | 78 |
| | 50.6% | 32.25 | 17.1% | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| إذا ظهر اسمك في صحيفة يمكن لمحرك البحث فهرستها وعرضها ضمن نتائج البحث للآخرين الذين يبحثون عنك | 204 | 110 | 71 | 2.35 | 0.772 | 78.3 |
| | 53% | 28.6% | 18.4% | | | |
| الاشتراك في مصدر إخباري وقراءة المقالات | 229 | 89 | 67 | 2.42 | 0.770 | 80.7 |
| | 59.5% | 23.1% | 17.4% | | | |
| استخدام أجهزة تتبع اللياقة البدنية يمكن أن يؤدي إلى جمع بياناتك | 195 | 137 | 53 | 2.37 | 0.714 | 79 |
| | 50.6% | 35.6% | 13.8% | | | |
| استخدام تطبيقات الرعاية الصحية كالتي تقيس معدلاتك الحيوية أو تساعد في عدّ خطواتك ومعرفة المسافة التي تقطعها وتحفظ من خلالها حالتك الطبية | 213 | 122 | 50 | 2.42 | 0.711 | 80.7 |
| | 55.3% | 31.7% | 13% | | | |
| سجلات البحث التي تجريها باستخدام محركات البحث عبر الإنترنت | 245 | 103 | 37 | 2.54 | 0.665 | 84.7 |
| | 63.6% | 26.85 | 9.6% | | | |
| الموافقة على ملفات تعريف الارتباط (ملفات الكوكيز) التي تطلبها المواقع والتطبيقات | 222 | 137 | 26 | 2.51 | 0.621 | 83.7 |
| | 57.7% | 35.6% | 6.8% | | | |
| إنشاء حساب على موقع باستخدام التسجيل السريع بحساب مواقع التواصل الاجتماعي أو حساب جوجل | 242 | 128 | 15 | 2.59 | 0.566 | 86.3 |
| | 62.95 | 33.25 | 3.9% | | | |
| التقط صديقك صورة لك ووضعها على صفحته الشخصية فقط دون أن يشير إليك | 128 | 159 | 98 | 2.08 | 0.763 | 69.3 |
| | 33.2% | 41.3% | 25.5% | | | |
| أشار إليك صديقك في منشوره الذي يتحدث فيه عنك لكنك تمنع مشاركة الآخرين منشورات على صفحتك | 189 | 138 | 58 | 2.34 | 0.726 | 78 |
| | 49.1% | 35.8% | 15.1% | | | |
| البحث عن المعلومات الخاصة بأفراد آخرين عبر الإنترنت دون إذنهم | 151 | 185 | 49 | 2.26 | 0.671 | 75.3 |
| | 39.2% | 48.1% | 12.7% | | | |
| نشر معلومات تخص شخص آخر دون إذن الشخص المعني | 163 | 154 | 68 | 2.25 | 0.735 | 75 |
| | 42.3% | 40% | 17.7% | | | |
| تسجيل الدخول إلى حسابك على المنصات المختلفة (مثل تسجيل الدخول لحساب جوجل) يحفظ إعداداتك المفضلة ومعلوماتك الشخصية | 197 | 134 | 54 | 2.37 | 0.718 | 79 |
| | 51.2% | 34.8% | 14% | | | |

تشير نتائج هذا الجدول (١٠) إلى إدراك المستخدم للأنشطة التي يعتقد أنها تعمل على تكوين بصمته الرقمية، ويعتقد المستخدمون أن في مقدمتها إنشاء حساب على موقع باستخدام التسجيل السريع بحساب مواقع التواصل الاجتماعي أو حساب جوجل بوزن

حسابي قدره ٨٦.٣%، يليه عملية الشراء التي يجريها عبر الإنترنت (العنصر الذي تم شراؤه، ومن أين تم الشراء، ومتى، وتكلفته، وطريقة الدفع...) بوزن حسابي ٨٥.٧%، وفي الترتيب الثالث نظام تحديد المواقع العالمي (GPS) وإشارات شبكة WIFI بوزن حسابي ٨٥.٣%، ثم كتابة منشور، أو مشاركة صورة، أو التعليق على منشور شخص آخر، أو الإعجاب بصفحة، أو متابعة صفحة أو شخص بمواقع التواصل الاجتماعي بوزن حسابي ٨٥%، يلي ذلك تفاعلاته في المنتديات والمدونات والمجتمعات عبر الإنترنت بوزن حسابي ٨٥%، ثم الصور ومقاطع الفيديو التي ينشرها بنفسه أو يحفظها عبر الإنترنت ٨٤.٧%، ثم سجلات البحث التي يجريها باستخدام محركات البحث عبر الإنترنت بوزن حسابي ٨٤.٧%، ثم إعطاء الأذونات للتطبيقات للوصول للمعلومات (مثل قائمة جهات الاتصال – موقعه الجغرافي...) ٨٣.٧%، ثم الموافقة على ملفات تعريف الارتباط (ملفات الكوكيز) التي تطلبها المواقع والتطبيقات ٨٣.٧%، ثم زيارة مواقع الويب وجلسات التصفح بها بوزن حسابي ٨٣.٣%، ثم تفاعلاته في التطبيقات أو المتصفحات بوزن حسابي ٨٢%، ثم عنوان IP الخاص به لتتبع نشاطه وجمع معلومات عن مكانك بوزن حسابي ٨١.٧%، ثم الاشتراك في مصدر إخباري وقراءة المقالات بوزن حسابي ٨٠.٧%، واستخدام تطبيقات الرعاية الصحية كالتي تقيس معدلاته الحيوية أو تساعد في عدّ خطواتك ومعرفة المسافة التي يقطعها وتحفظ من خلالها حالته الطبية ٨٠.٧%، ثم ملء نموذج تسجيل حساب جديد (سواء بموقع أو تطبيق أو شبكات التواصل الاجتماعي) بوزن حسابي ٧٩.٣%، ثم استخدام أجهزة تتبع اللياقة البدنية يمكن أن يؤدي إلى جمع بياناته بوزن حسابي ٧٩%، وتسجيل الدخول إلى حسابه على المنصات المختلفة (مثل تسجيل الدخول لحساب جوجل يحفظ إعداداته المفضلة ومعلوماته الشخصية) بوزن حسابي ٧٩%، ثم إذا ظهر اسمه في صحيفة يمكن لمحرك البحث فهرستها وعرضها ضمن نتائج البحث للآخرين الذين يبحثون عنه بوزن حسابي ٧٨.٣%، ثم البيانات البيومترية، مثل بصمات الأصابع والتعرف على الوجه ومسح قزحية العين، بوزن حسابي ٧٨%، ثم إشارة صديق في منشوره يتحدث فيه عن المستخدم لكنه يمنع مشاركة الآخرين منشورات على صفحته ٧٨%، ثم بيانات الحساب البنكي وبطاقة الائتمان التي وضعها

لأغراض مثل التسوق الإلكتروني أو المدفوعات الإلكترونية ٧٦.٧، ثم رسائل البريد الإلكتروني التي يرسلها ويستقبلها ٧٦%، ثم البحث عن المعلومات الخاصة بأفراد آخرين عبر الإنترنت دون إذنهم ٧٥.٣%، ثم نشر معلومات تخص شخصاً آخر دون إذن الشخص المعني بوزن حسابي ٧٥%، ثم التقاط صديقه صورة له ووضعها على صفحته الشخصية فقط دون أن يشير إليه بوزن حسابي ٦٩.٣%.

ويمكن تفسير النتائج على النحو الآتي: يأتي اعتقاد المستخدمين أن إنشاء حساب على موقع باستخدام التسجيل السريع بحساب مواقع التواصل الاجتماعي أو حساب جوجل يعمل على تكوين البصمة الرقمية في مقدمة الترتيب، وذلك انعكاس لإدراكه ما وراء محاولة المواقع أو التطبيقات من المحاولة الظاهرة للتيسير على المستخدم عبر إتاحة التسجيل بحسابه، والهدف الذي قد يكون مبطنًا؛ إذ يمكن أن يشارك الموقع أو الخدمة بعض معلوماته من حساب موقع التواصل الاجتماعي أو حساب جوجل ومشاركتها مع أطراف ثالثة أخرى، أو قد يتتبع نشاطه، وعلى الجانب الإيجابي يمكن أن يوثق هوية الفرد من خلال ربط حساباته ببعضها، وهو ما يعمل على تقوية بصمته الرقمية.

وتتضمن عملية الشراء عبر الإنترنت تفاصيل عديدة مهمة، تتمثل في وصف محدد للعنصر الذي تم شراؤه، ومصدر الشراء وتاريخه وتكلفته، والوسيلة المستخدمة للدفع، مما يجعلها تسهم في تحديد دقيق لاهتمامات الفرد كجزء من تشكيل ملف تعريف خاص به، ويشير غالبية المستخدمين إلى أن نظام تحديد المواقع العالمي من أهم الأنشطة التي تشكل بصمتهم الرقمية، لأنه يوفر معلومات جغرافية دقيقة لإحداثيات الجهاز المستخدم؛ تلك الأماكن التي ترسم تاريخًا لتنقلات الفرد ومساراته؛ وكثيراً ما يعاين المستخدم هذه الحالة عند استخدامه لتطبيقات، فعلى سبيل المثال، يمكن أن يحصل على معلومات الطقس المتعلقة بمكان وجوده؛ ليس فقط البلد، ولكن المنطقة التي يوجد بها، من خلال استشعار التطبيق لمكان وجوده دون تحديد المستخدم، وكذلك الأمر عند استخدام أحد مواقع التسوق التي لها نسخة مختلفة لكل بلد، فيستشعر الموقع المنطقة الجغرافية ويحدد واجهة الاستخدام وبيانات العملة واللغة بما يناسب دولة المستخدم، وغير ذلك، بما يوفر تجربة مخصصة وزيادة دقة توجيه المحتوى للمستخدم. وتمثل جميع هذه

الأنشطة بصمة رقمية نشطة؛ يصنعها المستخدم بنفسه، وبينما قد لا يحدد المستخدم بشكل استباقي وصول المواقع والتطبيقات لمكانه الجغرافي، إلا أن دوام تقبله لما ينتجه عنه من هذه الأذونات يعد تفريطًا في بيانات كان يمكنه التحكم فيها وتقليل الوصول إليها، وهو أيضًا ما تعتمد عليه شركات التكنولوجيا والاتصالات من تباطؤ المستخدم وإغفاله عن مراجعة الإعدادات الأساسية التي تختارها التطبيقات والمواقع له. كما أشار المستخدمون إلى أن كتابة منشور، أو مشاركة صورة، أو التعليق على منشور شخص آخر، أو الإعجاب بصفحة، أو متابعة صفحة أو شخص بمواقع التواصل الاجتماعي، إضافة إلى تفاعلاته في المنتديات والمدونات والمجتمعات عبر الإنترنت، والصور وسجلات البحث أيضًا، من ضمن أكثر الأنشطة التي تعمل على تشكيل البصمة الرقمية للمستخدمين، وهي أيضًا تعد بصمات نشطة، فالفرد بصفته متحكمًا فيما ينشره يفترض إدراكه أثر ذلك المتوقع عليه.

ويظهر أن أقل الأنشطة تشكيلًا للبصمة رقمية من وجهة نظر المستخدم هي غير المتعلقة بسلوكه الشخصي المباشر، فرغم أن البحث عن المعلومات الخاصة بأفراد آخرين عبر الإنترنت سيبقي في سجل بحث المستخدم وتصفحه، فإنه قد يعتقد أن المعلومات التي ستظهر لا تخصه، ومن ثم قد لا تُشكِّل بصمته الرقمية، كما يمكن أن يعتقد أن نشر معلومات أو صورة تخص شخصًا آخر دون إذن الشخص المعني لن تكون ظاهرة في سجل المستخدم الشخصي الخاص، وإنما يمكن أن تمثل أثرًا في سجل المستخدم الذي نشر، بينما في الحقيقة أن هذا النشر يمثل ظلًا رقمية قد تعمل على اتساع البصمة الرقمية في ظل التحليل الواسع لبيانات الأفراد.

**جدول (١١) مستوى معرفة المستخدمين بالأنشطة المكونة للبصمة الرقمية**

| المعرفة بالأنشطة المكونة للبصمة الرقمية | الإجمالى | |
|---|---|---|
| | ك | % |
| منخفض | 13 | 3.4% |
| متوسط | 134 | 34.8% |
| مرتفع | 238 | 61.8% |
| الإجمالي | 385 | 100% |

تشير نتائج الجدول السابق (١١) إلى مستوى معرفة الجمهور بالأنشطة المكونة للبصمة الرقمية، وقُدِّرت الإجابات وفقًا لمقياس ليكرت الثلاثي على النحو: موافق=3، محايد=2، غير موافق=1، ومن ثمَّ فإن محصلة المقياس تتكون من (٥١) درجة من ٢٥: ٧٥، مقسمة على ثلاثة مستويات: المستوى المنخفض (٢٥- ٤١)، المستوى المتوسط (٤٢- ٥٨)، المستوى المرتفع (٥٩-٧٥). ووفقًا لما ورد في الجدول، يظهر المبحوثون معرفة مرتفعة بالأنشطة التي تشكل البصمة الرقمية فقد كانت نسبته ٦١.٨%، بينما كان مستوى المعرفة لدى ٣٤.٨% متوسطًا، وكانت النسبة الأقل من المبحوثين لديهم معرفة منخفضة بالأنشطة المكونة للبصمة الرقمية بنسبة ٣.٤%. وتعكس هذه النتيجة معرفة واعية من المستخدم للإنترنت وتطبيقاتها المختلفة، وما يعمل منها على تشكيل البصمة الرقمية.

**جدول (١٢) تأثيرات البصمة الرقمية (الفائدة المتصورة/ والمخاطر المتوقعة)**

| الفوائد المتصورة | موافق | محايد | غير موافق | المتوسط | الإنحراف المعياري | الوزن النسبي |
|---|---|---|---|---|---|---|
| تساعد البصمة الرقمية في الحصول على محتوى مخصص لم أكن لأحصل عليه بطريقة أخرى | 242 | 91 | 52 | 2.49 | 0.722 | 83 |
| | %62.9 | 23.6% | 13.5% | | | |
| يمكن أن تساعد البصمة الرقمية في تعزيز فرصي وبناء سمعة إيجابية والشهرة عبر الإنترنت | 174 | 155 | 56 | 2.31 | 0.710 | 77 |
| | 45.2% | 40.3% | 14.5% | | | |
| يمكن أن تساعد البصمة الرقمية في منع عرض فئات حساسة من المحتوى لا تناسبني ومنع المحتوى غير المرغوب فيه | 183 | 128 | 74 | 2.28 | 0.767 | 76 |
| | 47.5% | 33.25% | 19.2% | | | |
| سيكون من الرائع أن تجمع الشركات بياناتي لفهم أسلوبي ومن ثم حمايتي من عمليات الاحتيال وإساءة الاستخدام | 191 | 118 | 76 | 2.30 | 0.778 | 76.7 |
| | 49.6% | 30.6% | 19.7% | | | |
| البصمة الرقمية تجعل من السهل العثور علي عبر الإنترنت وربط مهاراتي وإنجازاتي لشخصي | 87 | 120 | 178 | 2.24 | 0.796 | 74.6 |
| | 22.6% | 31.2% | 46.2% | | | |
| من الجيد أن تظهر المعلومات التي أشاركها في البيئة الرقمية في حياتي المهنية أو الخاصة في المستقبل | 166 | 152 | 67 | 2.26 | 0.735 | 75.3 |
| | 43.1% | 39.5% | 17.4% | | | |
| سيكون من الجيد مساعدة الشركات | 91 | 152 | 142 | 1.87 | 0.768 | 62 |

| الفوائد المتصورة | موافق | محايد | غير موافق | المتوسط | الإنحراف المعياري | الوزن النسبى |
|---|---|---|---|---|---|---|
| على تطوير خدمات أفضل من خلال تحليلهم لبياناتى | 23.6% | 39.5% | 36.9% | | | |
| يمكن لتسجيل أنشطتي في البيئات الرقمية أن يساعدني بشكل كبير في حياتي اليومية، مثل تذكر الأماكن التي أزورها ومشاركة التقويم والملاحظات والمستندات | 204 | 113 | 68 | 2.35 | 0.764 | 78.3 |
| | 53% | 29.4% | 17.7% | | | |
| من الجيد مراجعة أنشطتي على الإنترنت وتعديلها لتظهرني بصورة إيجابية | 176 | 159 | 50 | 2.33 | 0.694 | 77.7 |
| | 45.7% | 41.3% | 13% | | | |
| تساعد البصمة الرقمية في البحث والتقصى عن الآخرين رقميا | 155 | 152 | 78 | 2.20 | 0.753 | 73.3 |
| | 40.3% | 39.5% | 20.3% | | | |
| **المخاطر المتوقعة** | **موافق** | **محايد** | **غير موافق** | **المتوسط** | **الإنحراف المعيارى** | **الوزن النسبى** |
| يمكن أن أواجه عواقب سلبية بسبب بصمتى الرقمية وأن تستخدم ضدى | 197 | 138 | 50 | 2.38 | 0.705 | 79.3 |
| | 51.2% | 35.8% | 13% | | | |
| يمكن أن تفرط الجهات الرقمية في جمع معلوماتى وبياناتى | 209 | 105 | 71 | 2.36 | 0.775 | 78.7 |
| | 54.3% | 27.3% | 18.4% | | | |
| من المزعج والمقلق إغراقي باستمرار بالإعلانات والمحتوى المخصص | 204 | 127 | 54 | 2.39 | 0.721 | 79.7 |
| | 53% | 33% | 14% | | | |
| أخشى من إساءة استخدام المعلومات المخزنة لدى الجهات الرقمية المختلفة | 219 | 119 | 47 | 2.45 | 0.702 | 81.7 |
| | 56.9% | 30.9% | 12.2% | | | |
| أشعر بالقلق من تسريب بياناتي إلى وكالات خارجية دون إذنى | 203 | 130 | 52 | 2.39 | 0.714 | 79.7 |
| | 52.7% | 33.8% | 13.5% | | | |
| أشعر بالقلق من تعرض بياناتي للخطر بسبب خطأ من جامعيها | 208 | 118 | 59 | 2.38 | 0.738 | 79.7 |
| | 54% | 30.6% | 15.3% | | | |
| ربما أندم على الأشياء التي شاركتها في البيئات الرقمية ولا أستطيع محوها | 195 | 133 | 57 | 2.36 | 0.726 | 78.7 |
| | 50.6% | 34.5% | 14.8% | | | |
| البصمة الرقمية دائمة ومن الصعب محوها | 161 | 130 | 94 | 2.17 | 0.796 | 72.3 |
| | 41.8% | 33.8% | 24.4% | | | |
| أخشى من استخدام بصمتي الرقمية ضدي في المواقف الشخصية أو المهنية | 180 | 143 | 62 | 2.31 | 0.732 | 77 |
| | 46.8% | 37.1% | 16.1% | | | |
| من المقلق أن تساعد البصمة الرقمية الآخرين على التنبؤ بصفاتنا الخاصة التي لا نرغب في مشاركتها عبر الإنترنت | 189 | 143 | 53 | 2.35 | 0.711 | 78.3 |
| | 49.1% | 37.1% | 13.9% | | | |

تشير نتائج الجدول السابق (١٢) إلى كل من الفوائد المتصورة من البصمة الرقمية والمخاطر المتوقعة.

أولًا: الفوائد المتصورة: جاء في الترتيب الأول لاتجاهات المبحوثين فيما يخص الفوائد المتصورة أن البصمة الرقمية "تساعد في الحصول على محتوى مخصص لم يكن ليحصل عليه بطريقة أخرى (مثل إعلانات أكثر فائدة أو أشخاص يهمهم أمرهم بشدة)" بوزن نسبي ٨٣%، ثم "يمكن لتسجيل أنشطتي في البيئات الرقمية أن يساعدني بشكل كبير في حياتي اليومية مثل تذكر الأماكن التي أزورها ومشاركة التقويم والملاحظات والمستندات" بوزن نسبي ٧٨.٣%، ثم "من الجيد مراجعة أنشطتي على الإنترنت وتعديلها لتظهرني بصورة إيجابية" بوزن نسبي ٧٧.٧%، ثم "يمكن أن تساعد البصمة الرقمية في تعزيز فرصي وبناء سمعة إيجابية والشهرة عبر الإنترنت" بوزن نسبي ٧٧%، ثم "سيكون من الرائع أن تجمع الشركات بياناتي لفهم أسلوبي ومن ثم حمايتي من عمليات الاحتيال وإساءة الاستخدام" بوزن نسبي ٧٦.٧%، ثم "يمكن أن تساعد البصمة الرقمية في منع عرض فئات حساسة من المحتوى لا تناسبني ومنع المحتوى غير المرغوب فيه" بوزن نسبي ٧٦%، ثم "البصمة الرقمية تجعل من السهل العثور عليّ عبر الإنترنت وربط مهاراتي وإنجازاتي لشخصي" بوزن نسبي ٧٤.٦%، ثم "من الجيد أني أستطيع البحث والتقصي عن الآخرين رقميًا" بوزن نسبي ٧٣.٣%، ثم "سيكون من الجيد مساعدة الشركات على تطوير خدمات أفضل من خلال تحليلهم لبياناتي" بوزن نسبي ٦٢%.

ويمكن تفسير هذه النتائج على النحو الآتي: تعد المقايضة الإيجابية لبيانات الفرد العامل المؤثر في شعوره بعدم الممانعة لاتساع بصمته الرقمية، وأعلى إدراك للمنافع هو ما سيجنيه من محتوى مخصص لم يكن ليصل إليه بطريقة أخرى مثل الإعلانات الأكثر فاعلية، وهو ما يخدم المسوق أيضًا وليس المستخدم فقط، فيرفع من الكفاءة التسويقية له، والأشخاص الذين يهمه أمرهم، والموضوعات التي تلامس احتياجاته مباشرة دون أن يكلف نفسه عناء البحث، كما تعزز من تجربة التوصيات المخصصة للمستخدم، مثل منصات الترفيه كالموسيقى والأفلام. كما يمكن تعليل عدّ المستخدمين تسجيل أنشطتهم في البيئات الرقمية يمكن أن يساعدهم بشكل كبير في حياتهم اليومية في مرتبة متقدمة

من الفوائد؛ إذ يمكن تسجيل الأنشطة رقمياً من ضبط التنبيهات والإشعارات لضمان عدم النسيان (مثل ربط اجتماع مهم على موقع زووم بالتقويم، فيُنبه المستخدم عبر البريد الإلكتروني أو إشعارات التقويم)، كما يمكن أن يوثق ذكرياته وتجاربه ويشاركها مع الآخرين، ويحقق أيضاً عبر مشاركة الملاحظات والمستندات التواصل والتعاون بشكل فعّال مع الآخرين، مما يمكن أن يعمل على زيادة إنتاجية الفرد.

وبينما تُعدّ قدرة الفرد على مراجعة أنشطته وتعديلها ليظهر بصورة إيجابية من ضمن الفوائد المتصورة بقوة لدى المستخدمين؛ إلا أن الواقع ربما ينبئ بصعوبة ذلك، فعلى الرغم من إمكانية حذف المحتوى السلبي غير المرغوب فيه، الذي أنشأه في وقت سابق، فإنه قد يكون محفوظًا بصورة أو بأخرى بشكل دائم على الإنترنت، ناهيك عن غير ذلك من معلومات خفية لا يعي أنها قد تم تخزينها. لذلك ترى الباحثة ضرورة توجيه تركيز المستخدم نحو البدء في بناء صورة إيجابية عن ذاته، يُمكن أن تكون عبر تقديم مضامين إيجابية، سواء كانت صوراً أو فيديوهات أو مقالات، بما يعبر عن اهتماماته ويعكس شخصيته بشكل إيجابي، كما يمكنه مشاركة تحديثات إيجابية لإنجازاته، إضافة إلى تحرير الملف الشخصي والحسابات الخاصة به بمعلومات مُحدَّثة تعكس شخصيته بإيجابية، وبالتأكيد يمكنه ضبط إعدادات الخصوصية للتحكم بمن يمكنه رؤية أنشطته، وضبطها من أجل منع مستخدمين آخرين من الوصول لمعلومات بصمته الإيجابية... وما إلى ذلك.

وتفسر الباحثة اتجاه المبحوثين نحو فائدة "البحث والتقصي عن الآخرين رقمياً" بأنها انعكاس لاعتمادهم على الخوارزميات في تخصيص المحتوى (الفائدة الحاصلة على أعلى ترتيب في قناعته بالفوائد المتصورة)، فالمستخدم لن يسعى لبذل الجهد في البحث عن أصدقاء وزملاء يشتركون في اهتماماته إذا كان بإمكانه الحصول على ذلك عبر خوارزميات التخصيص، إلا في سياق بعض الاحتياجات الخاصة التي تدفعه إلى إجراء هذا التقصي، لذا كان في آخر اهتماماته المتصورة. ويمكن أن يعكس اتجاه المبحوثين نحو مساعدة الشركات على تطوير خدمات أفضل وتحسين تجربة المستخدم إلى قناعاتهم بملكية البيانات، بحيث لا يجب الاعتماد عليها في تطوير الشركات لأعمالهم.

ثانياً: المخاطر المتوقعة: جاء في الترتيب الأول عبارة "أخشى من إساءة استخدام المعلومات المُخزَّنة لدى الجهات الرقمية المختلفة" بوزن نسبي ٨١.٩%، ثم عبارات "من المزعج والمقلق إغراقي باستمرار بالإعلانات والمحتوى المخصص"، و"أشعر بالقلق من تسريب بياناتي إلى وكالات خارجية دون إذني"، و"أشعر بالقلق من تعرض بياناتي للخطر بسبب خطأ من جامعيها" بوزن نسبي ٧٩.٧% لكل منها، ثم "يمكن أن أواجه عواقب سلبية (مثل التحرش عبر الإنترنت أو التنمر الإلكتروني) بسبب بصمتي الرقمية" بوزن نسبي ٧٩.٣%، ثم "يمكن أن تفرط الجهات الرقمية في جمع معلوماتي وبياناتي" بوزن نسبي ٧٨.٧%، و"ربما أندم على الأشياء التي شاركتها في البيئات الرقمية ولا أستطيع محوها" بوزن نسبي ٧٨.٧%، و"من المقلق أن تساعد البصمة الرقمية الآخرين على التنبؤ بصفاتنا الخاصة التي لا نرغب في مشاركتها عبر الإنترنت" بوزن نسبي ٧٨.٣%، ثم "أخشى من استخدام بصمتي الرقمية ضدي في المواقف الشخصية أو المهنية" بوزن حسابي ٧٧%، ثم "البصمة الرقمية دائمة ومن الصعب محوها" بوزن حسابي ٧٢.٣%.

ويمكن تفسير ارتفاع قلق المستخدمين من إساءة استخدام المعلومات المُخزَّنة لدى الجهات الرقمية المختلفة بأنه انعكاس لقناعاتهم بملكية بياناتهم، فمن غير المناسب استخدام بياناتهم في أمور مثل مراقبة الأنشطة الاجتماعية، أو توجيه التأثير لقناعات سياسية، كما يمثل استغلال البصمة الرقمية للمستخدمين مخاطر منها التوجيه الإعلاني الزائد بما لا يناسب المستخدم ويشكل إزعاجاً كبيراً له، وهو ربما من التوجهات السائدة في البيئة الرقمية ويلمسه المستخدمون أثناء إبحارهم في الإنترنت، إضافة إلى إمكانية تعرض هذه الجهات القائمة على جمع البيانات إلى اختراق خارجي نتيجة خطأ لديها، لذا كانت من ضمن المخاوف المتقدمة لدى المستخدمين.

بينما حظيت استدامة البصمة الرقمية وصعوبة محوها بترتيب أخير للمخاوف التي يعتقدها المستخدمون تجاه بصمتهم الرقمية، وهو ترتيب يعكس قناعاتهم بإمكانية مراجعة أنشطتهم وتعديلها لتظهرهم بصورة إيجابية كفائدة متصورة. وترى الباحثة أن هذه النتيجة ربما تدلل على اهتمام الجمهور الأكبر بالبصمة النشطة، وما يظهره المستخدم بنفسه للآخرين، بينما لا يعنيه ما خفي عنهم طالما لا يقفز إلى سطح العلانية.

جدول (١٣) مستوى تأثيرات البصمة الرقمية (الفائدة المتصورة/ المخاطر المتوقعة)

| تأثيرات البصمة الرقمية | | ك | % |
|---|---|---|---|
| الفائدة المتصورة | منخفض | 18 | 4.7% |
| | متوسط | 202 | 52.5% |
| | مرتفع | 165 | 42.9% |
| | الإجمالي | 385 | %100 |
| المخاطر المتوقعة | منخفض | 3 | %0.8 |
| | متوسط | 183 | %47.5 |
| | مرتفع | 199 | %51.7 |
| | الإجمالي | 385 | %100 |

تشير نتائج الجدول السابق (١٣) إلى مستوى معرفة الجمهور بالفوائد المتصورة للبصمة الرقمية، وقُدِّرت الإجابات وفقًا لمقياس ليكرت الثلاثي: موافق=3، محايد=2، غير موافق=1 ، ومن ثمَّ فإن محصلة المقياس تتكون من (٢١) درجة من (١٠: ٣٠)، مقسمة على ثلاثة مستويات: المستوى المنخفض (١٠- ١٦)، المستوى المتوسط (١٧-٢٣)، المستوى المرتفع (٢٤-٣٠). ووفقًا لذلك، كانت أغلب مستويات المبحوثين نحو الفائدة المتصورة متوسطة بنسبة ٥٢.٥%، وبفارق ليس كبيراً كان مستوى الفائدة المتصورة مرتفعاً لدى 42.9%، وحوالي ٤.٧% من المبحوثين أظهروا مستويات منخفضة نحو الفوائد المتصورة للبصمة الرقمية.

بينما يوضح مستوى اعتقاد الجمهور بالمخاطر المتوقعة نتيجة البصمة الرقمية، وقُدِّرت الإجابات وفقًا لمقياس ليكرت الثلاثي: موافق=3، محايد=2، غير موافق=1، ومن ثمَّ فإن محصلة المقياس تتكون من (٢١) درجة من (١٠: ٣٠)، مقسمة على ثلاثة مستويات: المستوى المنخفض (١٠- ١٦)، المستوى المتوسط (١٧-٢٣)، المستوى المرتفع (٢٤-٣٠). ووفقًا لذلك، كان مستوى إدراك المخاطر المتوقعة للبصمة الرقمية مرتفعاً لدى ٥١.٧% من المبحوثين، ومتوسطًا لدى ٤٧.٥% من المبحوثين، بينما كان لدى ٠.٨% منخفضاً.

**جدول (١٤) أسلوب اتخاذ القرار بالإفصاح عن المعلومات**

| أسلوب اتخاذ القرار بالإفصاح عن المعلومات (القرار العقلاني) | موافق | محايد | غير موافق | المتوسط | الإنحراف المعياري | الوزن النسبي |
|---|---|---|---|---|---|---|
| أفضل جمع المعلومات الضرورية قبل استخدام أي تطبيق أو موقع أو منصة في البيئات الرقمية | 216 | 99 | 70 | 2.38 | .775 | 79.3 |
| | 56.1% | 25.7% | 18.2% | | | |
| أُقيِّم بدائل القرار بدقة قبل اتخاذ القرار النهائي وقبل أي خطوة سواء الكشف عن معلومات خاصة بي أو النقر على رابط ... | 215 | 121 | 49 | 2.43 | .708 | 81 |
| | 55.8% | 31.4% | 12.7% | | | |
| قبل أن أقرر استخدام موقع أو تطبيق ما أخصص وقتًا للتفكير في الإيجابيات والسلبيات | 200 | 124 | 61 | 2.36 | .741 | 78.7 |
| | 51.9% | 32.2% | 15.8% | | | |
| حماية بياناتي في البيئة الرقمية أهم أولوياتي أثناء اتخاذ قراراتي في البيئة الرقمية | 141 | 144 | 100 | 2.11 | .785 | 70.3 |
| | 36.6% | 37.4% | 26% | | | |
| **أسلوب اتخاذ القرار بالإفصاح عن المعلومات (القرار البديهي)** | **موافق** | **محايد** | **غير موافق** | **المتوسط** | **الإنحراف المعياري** | **الوزن النسبي** |
| أعتمد بشكل أساسي على مشاعري الداخلية وحدسي الأول في تحديد إذا كنت سأكشف عن معلومات عني أم لا | 156 | 140 | 89 | 2.17 | .780 | 72.3 |
| | 40.5% | 36.4% | 23.1% | | | |
| تخليت عن محاولة مواكبة الحلول لحماية بياناتي والتحقق من الإعدادات | 127 | 126 | 132 | 1.99 | .821 | 66.3 |
| | 33% | 32.7% | 34.3% | | | |
| لا أزعج نفسي بقضاء وقت كبير في فهم كيفية حماية البيانات على الإنترنت | 166 | 137 | 82 | 2.22 | .773 | 74 |
| | 43.1% | 35.6% | 21.3% | | | |
| لا فائدة من تكريس اهتمام كبير لحماية بياناتي الشخصية عبر الإنترنت | 136 | 112 | 137 | 2.00 | .843 | 66.7 |
| | 35.3% | 29.1% | 35.6% | | | |

تدلل نتائج الجدول السابق (١٤) على كيفية اتخاذ المبحوثين القرار بالإفصاح عن المعلومات، وكانت استجاباتهم على محور اتخاذ القرار العقلاني على النحو: "أُقيِّم بدائل القرار بدقة قبل اتخاذ القرار النهائي وقبل أي خطوة، سواء الكشف عن معلومات خاصة بي أو النقر علي رابط" بوزن نسبي ٨١%، ثم "أفضل جمع المعلومات الضرورية قبل استخدام أي تطبيق أو موقع أو منصة في البيئات الرقمية" بوزن نسبي ٧٩.٣%، ثم "قبل أن أقرر استخدام موقع أو تطبيق ما أخصص وقتًا للتفكير في الإيجابيات والسلبيات"

بوزن نسبي ٧٨.٦%، يلي ذلك "حماية بياناتي في البيئة الرقمية أهم أولوياتي أثناء اتخاذ قراراتي في البيئة الرقمية" بوزن نسبي ٧٠.٣%. بينما كان الوزن النسبي لمحور اتخاذ القرار البديهي على النحو: "لا أزعج نفسي بقضاء وقت كبير في فهم كيفية حماية البيانات على الإنترنت" بوزن نسبي ٧٤%، ثم "أعتمد بشكل أساسي على مشاعري الداخلية وحدسي الأول في تحديد إذا كنت سأكشف عن معلومات عني أم لا" بوزن نسبي ٧٢.٣%، ثم "لا فائدة من تكريس اهتمام كبير لحماية بياناتي الشخصية عبر الإنترنت" بوزن نسبي ٦٦.٧%، ثم "تخليت عن محاولة مواكبة الحلول لحماية بياناتي والتحقق من الإعدادات" بوزن نسبي ٦٦.٣%.

ووفقًا لما تقدم، فإن ترجيح القرارات، إما بأسلوب عقلاني أو اتخاذ القرار بأسلوب بديهي، نهجان مختلفان لاتخاذ القرارات، لأنهما يختلفان في كيفية تحليل المعلومات وبناء القرار، وتدلل هذه النتائج على سيادة القرار العقلاني والتفكير الجيد في ملكية البيانات وطريقة التحكم فيها، واتخاذ قرارات الإفصاح عن المعلومات عبر التحليل المنطقي المعلومات، والاستناد إلى الشواهد، وإعمال المنطق والتفكير في العواقب المحتملة من أجل الوصول إلى قرار سليم.

وبينما يشير القرار البديهي إلى السرعة وعدم الاستناد إلى المنطق، والميل نحو الانطباعات الشخصية والحدس والمشاعر الفورية دون تحليل منطقي، فإن المستخدم قد يضطر تحت ضغط بعض الظروف المحيطة إلى الاندفاع نحو اتخاذ القرارات البديهية من أجل السرعة في الاستخدام، مثلًا: الرغبة في الاستهلاك الفوري للمحتوى، أو استخدام تطبيق، فيوافق على أذونات السماح التي يطلبها، أو يتخطى قراءة سياسات الاستخدام المُطوّلة والانتقال إلى الموافقة العمياء من أجل استمرار الاستخدام، وأيضًا مثل: الحاجة الملحة إلى قراءة محتوى موقع قد انتهج سياسة إخفاء المحتوى بمربع كبير لإجبار المستخدم على اتخاذ القرار فيما يخص سياسات ملفات تعريف الارتباط، وهو ما قد يمثل للمستخدم وقتًا إضافيًا لفهم المطلوب الإفصاح عنه، فيختار عدم الانزعاج بكل ذلك والتعامل وفقًا لحدسه ومشاعره واحتياجاته.

ومن خلال حساب المتوسط التجميعي لمحور القرار العقلاني، فقد بلغ ٢.٣٢، بينما بلغ المتوسط التجميعي لمحور القرار البديهي ٢.٠٩، أي أن اتخاذ القرار بشكل عقلاني يغلب على اتخاذ القرار بطريقة بديهية.

**جدول (١٥) أسلوب اتخاذ القرار بحماية البصمة الرقمية**

| أسلوب اتخاذ القرار بحماية البصمة الرقمية | | ك | % |
|---|---|---|---|
| القرار العقلانى | منخفض | 21 | 5.5% |
| | متوسط | 187 | 48.6% |
| | مرتفع | 177 | 46% |
| | الإجمالي | 385 | 100% |
| القرار البديهى | منخفض | 67 | 17.4% |
| | متوسط | 187 | 48.6% |
| | مرتفع | 131 | 34% |
| | الإجمالي | 385 | 100% |

تشير نتائج الجدول السابق إلى مستويات أسلوب اتخاذ القرار لحاية البصمة الرقمية، ووفقًا لكل من محور القرار العقلاني ومحور اتخاذ القرار البديهي -كل على حدة-، قُدِّرت الإجابات وفقًا لمقياس ليكرت الثلاثي: موافق=3، محايد=2، غير موافق=1 ، ومن ثمَّ فإن محصلة كل مقياس تتكون من (٩) درجات من (٤: ١٢)، مقسمة على ثلاثة مستويات: المستوى المنخفض (٤- ٦)، المستوى المتوسط (٧-٩)، المستوى المرتفع (١٠-١٢). وكان مستوى اتجاهات العينة نحو المحور الأول (القرار العقلاني) متوسطًا بنسبة ٤٨.٦%، ثم نسبة كبيرة منهم ٤٦% لديهم مستوى مرتفع، بينما نسبة قليلة جدًا ٥.٥% كان مستوى اتخاذ القرار بالنسبة إليهم منخفضًا. أما استجابات المبحوثين لمحور (القرار البديهي) فكان مستوى اتجاهات المبحوثين أيضًا يميل نحو المستوى المتوسط بنسبة ٤٨.٦%، و٣٤% للمستوى المرتفع، و١٧.٤% للمستوى المنخفض.

## جدول (١٦) إدارة البصمة الرقمية

| آليات إدارة البصمة الرقمية | دائما | أحيانًا | نادرا | المتوسط | الإنحراف | الوزن النسبى |
|---|---|---|---|---|---|---|
| أحيانًا أعطي معلومات غير دقيقة أو مضللة عن نفسي (مثل تاريخ الميلاد) | 115 | 178 | 92 | 2.06 | .732 | 68.7 |
| | 29.9% | 46.2% | 23.9% | | | |
| أبحث عن نفسي في محركات البحث لأرى إذا كانت هناك معلومات ظاهرة عني وأسعى لتغيير ما لا يعجبني | 102 | 191 | 92 | 2.03 | .710 | 67.7 |
| | 26.5% | 49.6% | 23.9% | | | |
| أكون حذرا بشأن المحتوى الذي أنشره وأشاركه وأتحقق مما كتبته عدة مرات قبل أن أشاركه | 196 | 159 | 30 | 2.43 | .634 | 81 |
| | 50.9% | 41.3% | 7.9% | | | |
| الحد من كمية البيانات الشخصية التي أشاركها عن نفسي خاصة على المنصات العامة مثل تاريخ الميلاد وعنوان المنزل | 138 | 162 | 85 | 2.14 | .749 | 71.3 |
| | 35.85 | 42.1% | 22.1% | | | |
| أنشر كل ما هو إيجابي فقط | 153 | 157 | 75 | 2.20 | .743 | 73.3 |
| | 39.7% | 40.8% | 19.5% | | | |
| أحذف حساباتي الراكدة على المواقع التي لم أعد أستخدمها | 67 | 143 | 175 | 1.72 | .743 | 57.3 |
| | 17.4% | 37.1% | 45.5% | | | |
| أرفض تقديم معلومات عن نفسي أو إعطاء أذونات للمواقع أو التطبيقات التي لا علاقة لها بالمعاملة | 171 | 172 | 42 | 2.34 | .665 | 78 |
| | 44.4% | 44.7% | 10.9% | | | |
| أستخدم بريدًا إلكترونيًا مخصصًا لتسجيل حسابات جديدة على مواقع أرغب في الانضمام إليها ولا أقدم بياناتي الحقيقية | 106 | 167 | 112 | 1.98 | .753 | 66 |
| | 27.5% | 43.4% | 29.1% | | | |
| أقرأ خيارات السماح لملفات تعريف الارتباط وأقلصها قدر المستطاع | 100 | 158 | 127 | 1.93 | .766 | 64.3 |
| | 26% | 41% | 33% | | | |
| أتحقق دائمًا من خيارات الخصوصية بالمواقع والتطبيقات المختلفة لأعلم أذونات السماح التي تحظى بها وأُعدل ما لا يناسبني | 147 | 155 | 83 | 2.17 | .756 | 72.3 |
| | 38.2% | 40.3% | 21.6% | | | |
| أقرأ سياسات الاستخدام مهما كانت طويلة ولا أوافق عليها إلا بعد قراءتها كاملة | 107 | 119 | 159 | 1.86 | .821 | 62 |
| | 27.8% | 30.9% | 41.3% | | | |
| أسعى لفهم ما تجمعه عني المواقع من | 135 | 173 | 77 | 2.15 | .728 | 71.7 |

| آليات إدارة البصمة الرقمية | دائما | أحيانًا | نادرا | المتوسط | الإنحراف | الوزن النسبى |
|---|---|---|---|---|---|---|
| بيانات | 35.1% | 44.9% | 20% | | | |
| أحذف جميع ملفات تعريف الارتباط وسجل التصفح بانتظام | 146 | 162 | 77 | 2.18 | .741 | 72.7 |
| | 37.9% | 42.1% | 20% | | | |
| أحرص على إلغاء خاصية استخدام التطبيقات والبرامج لتتبع مكاني الحالي إلا عند الاستخدام | 174 | 157 | 54 | 2.31 | .705 | 77 |
| | 45.2% | 40.8% | 14% | | | |
| لا أستخدم حساب مواقع التواصل الاجتماعي للتسجيل في أي موقع أو تطبيق | 142 | 153 | 90 | 2.14 | .765 | 71.3 |
| | 36.9% | 39.7% | 23.4% | | | |
| أستخدم وضع التصفح المتخفي عند تصفح الويب | 123 | 181 | 81 | 2.11 | .721 | 70.3 |
| | 31.9% | 47% | 21% | | | |
| أُحدث التطبيقات وأنظمة تشغيل الهاتف بصورة دورية | 142 | 181 | 62 | 2.21 | .699 | 73.7 |
| | 36.9% | 47% | 16.1% | | | |
| أطلب من الآخرين عدم نشر صور أو فيديو أظهر به دون إذني | 158 | 153 | 74 | 2.22 | .746 | 74 |
| | 41% | 39.7% | 19.2% | | | |
| اطلب من شخص ما إزالة شيء نشره عني عبر الإنترنت إذا كان لا يناسبني ظهوره | 135 | 171 | 79 | 2.15 | .732 | 71.7 |
| | 351% | 44.4% | 20.5% | | | |
| لا أزور مواقع مشبوهة يمكن أن تسيء لصورتي إذا علم أحد بذلك عني | 209 | 120 | 56 | 2.40 | .729 | 80 |
| | 54.3% | 31.2% | 14.5% | | | |
| أقوم بتعيين حذف سجل نشاطي على الويب وفي التطبيقات بشكل تلقائي | 87 | 126 | 172 | 1.78 | .791 | 59.3 |
| | 22.6% | 32.7% | 44.7% | | | |
| أقوم بتعيين حذف سجل المواقع الجغرافية الخاص بالمسارات التي سلكتها والأماكن التي زرتها تلقائيا | 76 | 134 | 175 | 1.74 | .766 | 58 |
| | 19.7% | 34.8% | 45.5% | | | |
| أبحث عن كيفية إدارة الحساب غير النشط لتحديد ما سيحدث لبياناتي في حالة التوقف عن استخدام الخدمة | 70 | 145 | 170 | 1.74 | .747 | 58 |
| | 18.2% | 37.75 | 44.2% | | | |

تشير نتائج الجدول السابق (١٦) إلى مستوى إدارة المبحوثين للبصمة الرقمية، وكان الوزن النسبي لاستجابات المبحوثين على الوجه الآتي: حظيت عبارة "أكون حذراً بشأن المحتوى الذي أنشره وأشاركه وأتحقق مما كتبته عدة مرات قبل أن أشاركه" بأعلى

وزن نسبي ٨١%، ثم "لا أزور مواقع مشبوهة يمكن أن تسيء لصورتي إذا علم أحد بذلك عني" بوزن نسبي ٨٠%، ثم "أرفض تقديم معلومات عن نفسي أو إعطاء أذونات للمواقع أو التطبيقات التي لا علاقة لها بالمعاملة" بوزن نسبي ٧٨%، ثم "أحرص على إلغاء خاصية استخدام التطبيقات والبرامج لتتبع مكاني الحالي إلا عند الاستخدام" بوزن نسبي ٧٧%، ثم "أطلب من الآخرين عدم نشر صور أو فيديو أظهر به دون إذني" بوزن نسبي ٨٤%، ثم أُحدث التطبيقات وأنظمة تشغيل الهاتف بصورة دورية" بوزن نسبي ٧٣.٧%، ثم "أنشر كل ما هو إيجابي فقط" بوزن نسبي ٧٣.٣%، ثم "أحذف جميع ملفات تعريف الارتباط وسجل التصفح بانتظام" بوزن نسبي ٧٢.٧%، ثم "أتحقق دائمًا من خيارات الخصوصية بالمواقع والتطبيقات المختلفة لأعلم أذونات السماح التي تحظى بها وأُعدل ما لا يناسبني" بوزن نسبي ٧٢.٣%، ثم "أسعى لفهم ما تجمعه عني المواقع من بيانات" بوزن نسبي ٧١.٧%، وعبارة "أطلب من شخص ما إزالة شيء نشره عني عبر الإنترنت إذا كان لا يناسبني ظهوره" بوزن نسبي ٧١.٧%، ثم "أُقيِّد كمية البيانات التي أشاركها عن نفسي كأن أخفي ملفي الشخصي عن العامة" بوزن نسبي ٧١.٣%، وعبارة "لا أستخدم حساب مواقع التواصل الاجتماعي للتسجيل في أي موقع أو تطبيق" بوزن نسبي ٧١.٣%، ثم "أستخدم وضع التصفح المتخفي عند تصفح الويب" بوزن نسبي٧٠.٣%، ثم "أحيانًا أعطي معلومات غير دقيقة أو مضللة عن نفسي (مثل تاريخ الميلاد)" بوزن نسبي ٦٨.٧%، ثم "أبحث عن نفسي في محركات البحث لأرى إذا كانت هناك معلومات ظاهرة عني وأسعى لتغيير ما لا يعجبني" بوزن نسبي ٦٧.٧%، ثم "أستخدم بريدًا إلكترونيًا مخصصًا لتسجيل حسابات جديدة على مواقع أرغب في الانضمام إليها ولا أقدم بياناتي الحقيقية" بوزن نسبي ٦٦%، ثم "أقرأ خيارات السماح لملفات تعريف الارتباط وأُقلصها قدر المستطاع" بوزن نسبي ٦٤.٣%، ثم "أقرأ سياسات الاستخدام مهما كانت طويلة ولا أوافق عليها إلا بعد قراءتها كاملة" بوزن نسبي ٦٢%، ثم "أقوم بتعيين حذف سجل نشاطي على الويب وفي التطبيقات بشكل تلقائي" بوزن نسبي ٥٩.٣%، ثم "أقوم بتعيين حذف سجل المواقع الجغرافية الخاص بالمسارات التي سلكتها والأماكن التي زرتها تلقائيًا" بوزن نسبي ٥٨%، وعبارة "أبحث عن كيفية إدارة

الحساب غير النشط لتحديد ما سيحدث لبياناتي في حال التوقف عن استخدام الخدمة" بوزن نسبي ٥٨%، ثم "أحذف حساباتي الراكدة على المواقع التي لم أعد أستخدمها" بوزن نسبي ٥٧.٣%.

وتتفق هذه النتائج مع نتائج دراسة (محمود محمد، ٢٠٢٢)[89]، التي أشارت إلى اطلاع حوالي ٣٥% فقط من المستخدمين على سياسة الاستخدام في مواقع التسويق الإلكتروني التي يترددون عليها، كما اتفقت معها في عدم الاعتداد بأسلوب تقديم بيانات خاطئة وسيلة للدفاع عن الخصوصية. وتتفق النتائج أيضًا مع نتائج دراسة (هدير أحمد، ٢٠٢٢)، التي أشارت إلى ارتفاع مستوى الاهتمام بضبط إعدادات الخصوصية، فقد كان مستوى الاهتمام بضبط الإعدادات متوسطًا بنسبة ٥.٤٤% يليه المستوى المرتفع بنسبة ٥.٤٠%، مما يعكس وعي المرأة بضبط إعدادات الأمان وتأمين حسابها. كما تتفق أيضًا مع دراسة (غادة النشار، ٢٠١٨)[90]، بارتفاع مستوى فهم إعدادات الأمان على موقع فيسبوك.

ويمكن تفسير هذه النتائج بسيادة إدارة البصمة الرقمية من خلال تحكم الفرد في بصمته النشطة، وعلى رأسها أن يكون حذرًا بشأن المحتوى الذي ينشره ويشاركه عبر الإنترنت، وعدم زيارة مواقع مشبوهة؛ إذ يهتم المستخدمون بالحفاظ على سمعة رقمية إيجابية نظرًا لأن أي محتوى غير مناسب قد يؤدي إلى الإضرار بسمعته الرقمية، التي تعد امتدادًا لسمعته في الواقع، كما أن مشاركة معلومات سلبية أو حساسة عن الآخرين يمكن أن تضر بالناشر مثلما تضر بالشخص المعني، هذا الحذر المحمود في ما ينشره المستخدمون يمكن أن ينعكس بإيجابية على فرصه المهنية وعلى علاقاته الاجتماعية. كما ينتج عن عدم زيارة مواقع مشبوهة الحفاظ على الخصوصية ومنع الاحتيال والاستغلال، لأن بعض المواقع مصممة من أجل الاحتيال (مثل المواقع التي تقدم برامج غير أصلية، والمواقع غير المرخصة التي تقدم الموسيقى والأفلام؛ فالمستخدم يتتبع الروابط التي تشير إليها المواقع أملًا في الحصول على هذه الخدمات غير الرسمية، مما قد يوقعه في فخ النقر على روابط مشبوهة قد تضع ملفات تعريف الارتباط أو برمجيات خبثيه على أجهزة المستخدم دون علمه هدفها اختراق الأجهزة والأنظمة، ويبقى المستخدم ساعيًا

خلف هذا العبث الرقمي والروابط المتدفقة في نوافذ منبثقة أمامه دون وعي بما يحدث في الخلفية).

كما يمكن تفسير وجود أغلب الخيارات الرامية إلى التحكم الأكثر تعقيدًا، التي تشير إلى ضرورة وجود معرفة متقدمة لدى المستخدم لإدارة بصمته الرقمية، في ترتيب متأخر، مثل إدارة الحسابات غير النشطة، وتعيين الحذف التلقائي للسجلات، لأنها تتطلب قدراً من الوعي المعلوماتي لدى المستخدم بوجود مثل هذه الخيارات أولًا، ثم امتلاكه القدرة على البحث عنها وفهمها واستيعابها، ومن ثم التجريب حتى الوصول لتعديل الخيارات بما يناسب احتياجاته. ويمكن تعليل ذلك بتشعب هذه المعلومات وتعقد الإعدادات وصياغتها أحيانًا بطريقة فنية، كما أنها قد تختلف من منصة لأخرى، ومن موقع لآخر، ومن خدمة لأخرى... وما إلى ذلك، ما مما يصعب على المستخدمين الوصول إلى الخيارات وفهمها، وقد لا توفر بعض شركات التكنولوجيا والاتصالات هذه التوجيهات والمعلومات والسياسات. إضافة إلى غياب التوجيه العام من المنصات حول كيفية الاستفادة من هذه الخيارات، وأيضًا يمكن أن تعزى هذه النتيجة إلى الرفض الثقافي من المستخدمين لاتخاذ قرارات حماية متكاملة وفعَّالة، خاصة إذا ساد الاعتقاد لديهم بعدم الاحتياج إلى حماية بياناتهم لعدم أهميتها، دون إدراك التأثيرات الشاملة.

**جدول (١٧) مستوى إدارة في البصمة الرقمية**

| إدارة البصمة الرقمية | الإجمالى | |
|---|---|---|
| | ك | % |
| منخفض | 11 | 2.9 |
| متوسط | 289 | 75.1 |
| مرتفع | 85 | 22.1 |
| الإجمالي | 385 | 100 |

يدلل الجدول السابق (١٧) على مستوى إدارة البصمة الرقمية للمبحوثين، وقُدِّرت الإجابات وفقًا لمقياس ليكرت الثلاثي: موافق=3، محايد=2، غير موافق=1، ومن ثمَّ فإن محصلة المقياس تتكون من (٥١) درجة من ٢٥: ٧٥، مقسمة على ثلاثة مستويات: المستوى المنخفض (٢٥ – ٤٢) المستوى المتوسط (٤٣-٦٠)، المستوى المرتفع (٦١-٧٥). ويعني ذلك أن مستوى إدارة المستخدمين لبصمتهم الرقمية متوسط؛ إذ كان أغلب المبحوثين في فئة

المتوسط من المقياس بنسبة ٧٥.١%، بينما كان مستوى إدارة البصمة الرقمية لدى ٢٢.١% منهم مرتفعاً، ونسبة قليلة بلغت ٢.٩% كان مستوى إدارتهم لبصمتهم الرقمية منخفضاً.

**اختبار الفروض:**

**الفرض الأول: توجد علاقة ارتباطية بين مستوى الوعى بالبصمة الرقمية وفقاً للمتغيرات الديموغرافية (النوع والعمر).**

اختُبرت صحة هذا الفرض بإيجاد قيمة (ت) لمعرفة العلاقة بين مستوى الوعي بالبصمة الرقمية وكل من الذكور والإناث، وإيجاد قيمة (ف) لمعرفة العلاقة بين مستوى الوعي بالبصمة الرقمية والفئات العمرية المختلفة لأفراد العينة. وهو ما يلاحظ في الجدولين الآتيين:

**جدول (١٨) الفروق بين الذكور والإناث في درجة الوعى بالبصمة الرقمية**

| | النوع | العدد N | المتوسط الحسابى Mean | الانحراف المعياري | قيمة T | درجات الحرية df | مستوى المعنوية Sig |
|---|---|---|---|---|---|---|---|
| الوعى بالبصمة الرقمية | أنثى | 236 | 2.4280 | .49584 | 0.465 | 383 | 0.643 |
| | ذكر | 149 | 2.4027 | .55653 | | | |

تشير نتائج اختبار (ت) في الجدول السابق إلى دلالة الفروق بين الذكور والإناث في الوعي بالبصمة الرقمية، وقد بلغت قيمة (ت) ٠.٤٦٥، عند مستوى معنوية ٠.٦٤٣، وهي غير دالة، أي أنه لا توجد فروق وفقاً للنوع بين الذكور والإناث في درجة الوعي بالبصمة الرقمية.

**جدول (١٩) الفروق في الوعى بالبصمة الرقمية بين المبحوثين وفقاً لمتغير العمر**

| | العمر | العدد N | المتوسط الحسابى Mean | الانحراف المعياري | درجات الحرية Df | قيمة F | مستوى المعنوية Sig |
|---|---|---|---|---|---|---|---|
| الوعى بالبصمة الرقمية | أقل من 21 عاماً | 88 | 2.4886 | .52510 | 3 381 | 2.121 | 0.097 |
| | من21 إلى أقل من 30عاماً | 114 | 2.4474 | .53368 | | | |
| | من30 إلى أقل من 40عاماً | 108 | 2.4167 | .51383 | | | |
| | 40 عاماً فأكثر | 75 | 2.2933 | .48695 | | | |
| | المجموع | 385 | 2.4182 | .51960 | | | |

تشير نتائج اختبار (ف) إلى عدم وجود فروق ذات دلالة إحصائية في مستوى الوعي بالبصمة الرقمية، فقد بلغت قيمة (F) ٢،١٢١، وهي غير دالة إحصائيًا، أي أنه لا توجد فروق وفقًا لمتغير العمر في الوعي بالبصمة الرقمية. **ووفقًا لذلك لم يثبت وجود علاقة بين مستوى الوعى بالبصمة الرقمية بين المبحوثين وفقًا لمتغيري النوع والعمر.**

**الفرض الثانى: توجد علاقة ارتباطية دالة إحصائيا بين مستوى المعرفة بالأنشطة المكونة للبصمة الرقمية وفقًا للمتغيرات الديموغرافية (النوع والعمر).**

اختُبرت صحة هذا الفرض بإيجاد قيمة (ت) لمعرفة دلالة العلاقة بين مستوى المعرفة بالأنشطة المكونة للبصمة الرقمية بين الذكور والإناث، واختبار (ف) لمعرفة إذا كانت توجد علاقة وفقًا لمتغير العمر، وذلك على النحو الآتي:

**جدول (٢٠) الفروق بين الذكور والإناث في المعرفة بالأنشطة المكونة للبصمة الرقمية**

| المعرفة بالأنشطة المكونة للبصمة الرقمية | النوع | العدد N | المتوسط الحسابى Mean | الانحراف المعياري | قيمة T | درجات الحرية df | مستوى المعنوية Sig |
|---|---|---|---|---|---|---|---|
| | أنثى | 236 | 2.5551 | .56975 | 1.300 | 383 | 0.054 دال |
| | ذكر | 149 | 2.6309 | .53712 | | | |

تشير نتائج اختبار (ت) في الجدول السابق، حول العلاقة بين الذكور والإناث والمعرفة بالأنشطة التي تعمل على تشكيل البصمة الرقمية، إلى أن قيمة (ت) بلغت ١.٣٠٠، عند مستوى معنوية ٠.٠٥٤، وهي دالة، أي أنه توجد فروق وفقًا للنوع بين الذكور والإناث في مستوى المعرفة بالأنشطة المكونة للبصمة الرقمية لصالح الذكور؛ إذ كان المتوسط الحسابي لمقدار المعرفة بالأنشطة المكونة للبصمة الرقمية للذكور ٢.٦٣، وبالنسبة للإناث ٢.٥٥.

**جدول (٢١) معرفة المستخدمين بالأنشطة المكونة للبصمة الرقمية وفقًا لمتغير العمر**

| | العمر | العدد N | المتوسط الحسابى Mean | الانحراف المعياري | درجات الحرية Df | قيمة F | مستوى المعنوية Sig |
|---|---|---|---|---|---|---|---|
| المعرفة بالأنشطة المكونة للبصمة الرقمية | أقل من 21 عامًا | 88 | 2.5909 | .51721 | 3<br>381 | 0.583 | 0.626<br>غير دال |
| | من21 إلى أقل من 30عامًا | 114 | 2.5526 | .56587 | | | |
| | من30 إلى أقل من 40عامًا | 108 | 2.6389 | .58738 | | | |
| | 40 عامًا فأكثر | 75 | 2.5467 | .55247 | | | |
| | المجموع | 385 | 2.5844 | .55787 | | | |

تشير نتائج اختبار (ف) إلى عدم وجود فروق ذات دلالة إحصائية في مستوى المعرفة بالأنشطة المكونة للبصمة الرقمية؛ إذ بلغت قيمة (F) ٠.٥٨٣، وهي غير دالة إحصائيًا، أي أنه لا توجد فروق وفقًا لمتغير العمر في المعرفة بالأنشطة المكونة للبصمة الرقمية.

**وتأسيسًا على ما تقدم في الجدولين السابقين، تثبت صحة الفرض جزئيا فيما يخص متغير النوع.**

**الفرض الثالث: توجد علاقة ارتباطية دالة إحصائيا بين مستوى إدارة بالبصمة الرقمية لدى المبحثوين وفقًا لمتغيري النوع والعمر.**

اختُبرت صحة هذا الفرض بإيجاد قيمة (ت) لمعرفة دلالة العلاقة بين مستوى إدارة البصمة الرقمية بين الذكور والإناث، واختبار (ف) لمعرفة إذا كانت توجد علاقة وفقًا لمتغير العمر، وذلك على النحو الآتي:

**جدول (٢٢) الفروق بين الذكور والإناث في إدارة البصمة الرقمية**

| | النوع | العدد N | المتوسط الحسابى Mean | الانحراف المعياري | قيمة T | درجات الحرية df | مستوى المعنوية Sig |
|---|---|---|---|---|---|---|---|
| مستوى إدارة البصمة الرقمية | أنثى | 236 | 2.2246 | .45708 | 1.737 | 383 | 0.083<br>غير دال |
| | ذكر | 149 | 2.1409 | .46528 | | | |

تشير نتائج اختبار (ت) في الجدول السابق، حول دلالة الفرق بين الذكور والإناث في إدارة التحكم بالبصمة الرقمية، إلى أن قيمة (ت) بلغت ١.٧٣٧، عند مستوى معنوية ٠.٠٨٣، وهي غير دالة، أي أنه لا توجد فروق وفقًا للنوع بين الذكور والإناث في مستوى التحكم بالبصمة الرقمية.

**جدول (٢٣) إدارة البصمة الرقمية وفقًا لمتغير العمر**

| | العمر | العدد N | المتوسط الحسابى Mean | الانحراف المعياري | درجات الحرية df | قيمة F | مستوى المعنوية Sig |
|---|---|---|---|---|---|---|---|
| مستوى إدارة البصمة الرقمية | أقل من 21 عامًا | 88 | 2.2955 | .45886 | 3<br>381 | 2.657 | 0.048<br>دال |
| | من21 إلى أقل من 30عامًا | 114 | 2.1140 | .45620 | | | |
| | من30 إلى أقل من 40عامًا | 108 | 2.2037 | .48836 | | | |
| | 40 عامًا فأكثر | 75 | 2.1733 | .41503 | | | |
| | المجموع | 385 | 2.1922 | .46148 | | | |

تشير نتائج اختبار F إلى وجود فروق ذات دلالة إحصائية في مستوى التحكم بالبصمة الرقمية؛ إذ بلغت قيمة (F) ٠.٠٤٨، وهي دالة إحصائيًا، أي أنه توجد فروق وفقًا لمتغير العمر في مستوى التحكم بالبصمة الرقمية لصالح الفئة العمرية الأصغر سنًا.

**وتأسيسا على ما تقدم في الجدولين السابقين، تثبت صحة الفرض جزئيا فيما يخص متغير العمر.**

**الفرض الرابع: توجد علاقة ارتباطية بين وعى المستخدمين بالبصمة الرقمية ومستوى إدارة البصمة الرقمية.** وللتحقق من صحة هذا الفرض استُخدم معامل بيرسون للارتباط، ويوضح الجدول الآتي نتيجة هذا الإجراء:

جدول (٢٤) العلاقة بين وعي المستخدمين بالبصمة الرقمية وإدارتها

| | | وعى الأفراد بالبصمة الرقمية |
|---|---|---|
| إدارة البصمة الرقمية | معامل الارتباط | .283 |
| | مستوى المعنوية | .055 |
| | ن | 385 |

تشير نتائج اختبار معامل بيرسون للارتباط إلى وجود علاقة ارتباط طردية بين وعي المستخدمين بالبصمة الرقمية ومستوى التحكم فيها؛ إذ بلغ معامل بيرسون ٠.٢٨٣ عند مستوى معنوية ٠.٠٥٥، وهي غير دالة، أي لا توجد علاقة بين وعي المستخدمين بالبصمة الرقمية ومستويات إدارتهم لها.

**مناقشة النتائج:**

لشركات التكنولوجيا والاتصالات الكبرى دور محوري في تمكين مختلف جوانب حياة الناس، فقد أصبحت السمة التكنولوجية هي السائدة في القرن الحالي؛ إذ تتم الاتصالات وتنتشر المعرفة وتصاغ الأفكار على نحو اعتيادي في بيئة رقمية، وقد وضحت النتائج انغماس المستخدمين لفترات زمنية بشكل يومي في استخدام الإنترنت، واستهلاك مجموعة واسعة من الأجهزة الذكية، على رأسها الهواتف الذكية وأجهزة الكمبيوتر المحمولة، واستخدام كثيف للشبكات الاجتماعية وتطبيقات المراسلة ومحركات البحث. ونظراً لأن توليد إيرادات الشركات يعتمد على آليات خوارزمية تتبع الإجراءات والسلوكيات الخاصة بالمستخدمين، وتسجل البيانات، وتدمج آثار وجودهم على الإنترنت في ملف شخصي متكامل، وقد تمكن من تبادل البيانات بين مختلف الكيانات المهتمة ببناء هذه الملفات، ولما كانت البنى التحتية الرقمية تستضيف عمليات تفاعل الأفراد في البيئة الرقمية، وفي ظل صعوبة إسناد حماية البيانات إلى القوانين والتشريعات وحدها في هذا الفضاء الافتراضي؛ توفر نتائج هذه الدراسة أدلة لدعم النظر إلى وعي الأفراد بوصفه أداة داعمة للتحكم في آثاره الرقمية، لا سيما مع وجود معلومات يمكن أن تكون حساسة بالنسبة للمستخدمين، مثل المعلومات المالية والحسابات المصرفية، والصور والفيديوهات الشخصية للمستخدم، وكذلك نشاط البريد الإلكتروني.

ولأن جميع المعلومات الشخصية لا تحمل درجة الأهمية نفسها، فإن بعض المعلومات يمكن الكشف عنها أو حجبها وفقًا للعواقب المتصورة إزاء هذا الإفصاح وإتاحة البيانات، لذا تظهر أهمية وزن القرارات وتطوير الأفراد لقواعد الخصوصية بما يتناسب مع احتياجاتهم.

وقد بيَّنت النتائج اعتقاد المبحوثين بالمدد الزمنية التي يمكن السماح لجهات تجميع بياناتهم أن يحتفظوا بها، فقد كان الاعتقاد السائد هو عدم المانعة، فلم تظهر الاستجابات مستوى كبيراً من القلق تجاه الحفاظ على بصمتهم الرقمية، ولم يتجه كثيرون بشكل قوي نحو خيارات منع أي جهنة من جمع البيانات، ورغم ذلك، ظهر اتجاه شائع بين الأفراد في العينة بالمحافظة على بياناتهم لفترة زمنية محدودة، قد تمتد إلى بضعة أسابيع أو شهور.

كما بيَّنت النتائج وجود قدر معقول من الوعي لدى المبحوثين بالبصمة الرقمية (٥٥.٦% الوعي بنسبة متوسطة، و٤٣.١% لديهم وعي بنسبة مرتفعة)، كما أن لدى المستخدمين معرفة جيدة بالأنشطة التي تعمل على تشكيل البصمة الرقمية (٦١.٨% معرفة بصورة مرتفعة، و٣٤.٨% معرفة بصورة متوسطة)، وكان على رأسها إنشاء حسابات باستخدام التسجيل السريع بحساب مواقع التواصل الاجتماعي أو حساب جوجل، وعمليات الشراء التي يجريها عبر الإنترنت، وتحديد موقعه الجغرافي عبر نظام تحديد المواقع العالمي (GPS) ، وإشارات شبكةWIFI . ويمكن القول أن النتائج الإيجابية التي يستشعرها الفرد إزاء المحتوى المخصص الذي لم يكن ليصل إليه بطريقة أخرى، والتوصيات حول الأفراد والموضوعات الملامسة لاحتياجاته؛ ترفع من قناعته بإيجابية البصمة الرقمية، وتؤدي إلى عدم المانعة في اتساع بصمته الرقمية.

فيما يمكن الإشارة إلى بعض المعضلات المعرفية التي قد تؤثر في مستوى أمان بياناتهم، وأهمها عدم قراءة سياسة الخصوصية والإعدادات؛ لذلك تمثل عملية الموافقة العمياء على سياسات الاستخدام وشروطه إجراء بديهياً بالنسبة إليهم من أجل الحصول على الخدمة، بما لا يعكس سيطرة حقيقية على البيانات. كما أوضحت النتائج أن

المستخدمين يفتقرون إلى القدرة على اتخاذ الخيارات التي تحتاج إلى وعي معلوماتي أكبر.

ورغم ما وفَّرته الإنترنت من فرص هائلة للأفراد لتقديم أنفسهم بطرق مختلفة؛ فإن بإمكانهم تعزيز الذات أو الاحتيال وتزوير معلومات الهوية، سواء لاعتقادهم أنها وسيلة لحماية الخصوصية أو لتحقيق دوافع ما، وهو ما قد يجعل شركات التكنولوجيا والاتصالات أكثر اعتماداً على البصمة السلبية غير النشطة من الأخرى النشطة لصعوبة تزييفها من قبل المستخدمين.

وفي ضوء ما تقدم، توصي الدراسة بمجموعة من الإجراءات ينبغي أن يُركِّز عليها المستخدم، ويمكن للجهات المعنية بدعم وتنمية المهارات الرقمية وضعها في الاعتبار:

- ضرورة تثقيف المستخدمين حول البيانات الرقمية وتأثير اتساع بصمتهم الرقمية ونتائج موافقتهم على استخدام الجهات المختلفة لبياناتهم.
- تأكيد أهمية بحث الفرد عن نفسه عبر محركات البحث بالاسم أو البريد الإلكتروني أو حسابات مواقع التواصل الاجتماعي، بوصفها خطوة أساسية لمعرفة المنشور عنه ويستطيع الآخرون معرفته، وهو ما يمكن أن يؤثر في مستقبله الشخصي أو المهني، ثم العمل على تقليل الآثار السلبية التي يجدها.
- توجيه الفرد نحو العناية بما يشاركه، والتفكير الجيد قبل النشر للمحافظة على بصمة إيجابية، وكذلك أخذ الحذر والحيطة مما قد ينشره الآخرون عنه ويمثل بصمة سلبية أو ما يعرف بالظلال الرقمية.
- الحد من استهلاك مصادر رقمية تسعى لرصد كثير من بياناتهم وسلوكهم، مما يؤدي إلى اتساع بصمتهم الرقمية، والاعتماد عوضاً عن ذلك على المواقع والتطبيقات التي لا تطلب معلومات شخصية عديدة، ولا تطلب أذونات سماح لعديد من البيانات.
- تنمية المهارات الرقمية عبر مراجعة إعدادات الخصوصية وسياسات ملفات التتبع والارتباط، والتأكد أنها مناسبة لما يعتقد أنه يلبي الاحتياجات دون إفراط.

- استخدام شبكات آمنة، مثل شبكة VPN تقوم على إخفاء عنوان بروتوكول الإنترنت الخاص بالمستخدم IP، مما يمنع تتبع نشاطه وتأمين اتصاله، كما من شأنها منع المواقع من تنزيل ملفات تعريف الارتباط على جهازه دون علمه.
- غالبًا ما تحمل التحديثات الأخيرة لأنظمة التشغيل والتطبيقات والمتصفحات تحديثًا، ليس فقط على مستوى واجهة الاستخدام والأدوات، ولكنها تعمل على تحديث الحلول وسدّ الثغرات في الأنظمة والبرامج وهو من شأنه منع هجمات المتسللين.
- ضرورة حذف الحسابات الراكدة على المواقع المختلفة، التي لم يعد المستخدم بحاجة إليها.

**قائمة المراجع:**


(1) Zuboff, S. (2022). Surveillance capitalism or democracy? The death match of institutional orders and the politics of knowledge in our information civilization. Organization Theory, 3(3), 26317877221129290.

(2) Tomasello, F. (2023). From industrial to digital citizenship: rethinking social rights in cyberspace. Theory and society, 52(3), 463-486.

(3) Montag, C., Lachmann, B., Herrlich, M., & Zweig, K. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. International journal of environmental research and public health, 16(14), 2612.

(4) Council of Europe (2014). Recommendation CM/ Rec (2014) 6 of the Committee of Ministers to member States on a Guide to human rights for Internet users. (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies).

(5) Buchanan, R., Southgate, E., & Smith, S. P. (2019). 'The whole world's watching really': Parental and educator perspectives on managing children's digital lives. Global Studies of Childhood, 9(2), 167-180.

(6) Chalklen, C., & Anderson, H. (2017). Mothering on Facebook: Exploring the privacy/openness paradox. Social Media+ Society, 3(2), 2056305117707187.

(7) Buchanan, R., Southgate, E., Smith, S. P., Murray, T., & Noble, B. (2017). Post no photos, leave no trace: Children's digital footprint management strategies. E-learning and digital Media, 14(5), 275-290.

(8) Marinelli, A., & Parisi, S. (2022). Apps, Platforms, and Everyday Practices: How People Perceive and Care (or not) About the Digital Traces They Leave Online. American Behavioral Scientist, 00027642221144852.
(9) The Australian Communications and Media Authority, Digital Footprints and Identities, Retrieved from: www.acma.gov.au/theACMA/Library/researchacma. Date: 12-10-2020.
(10) Camacho, M., Minelli, J., & Grosseck, G. (2012). Self and identity: raising undergraduate students' awareness on their digital footprints. Procedia-Social and Behavioral Sciences, 46, 3176-3181.
(11) Holloway, D. (2019). Surveillance capitalism and children's data: the Internet of toys and things for children. Media International Australia, 170(1), 27-36.
(12) Montag, C., & Elhai, J. D. (2023). On Social Media Design (Online-) Time Well-spent and Addictive Behaviors in the Age of Surveillance Capitalism. Current Addiction Reports, 1-7.
(13) Montag, C., Lachmann, B., Herrlich, M., & Zweig, K. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. Op. Cit.
(14) Michael, M., & Lupton, D. (2017). 'Depends on who's got the data': public understandings of personal digital dataveillance.
(15) Di Bene, E. (2022). Online Privacy: a Qualitative Inquiry About Privacy Perceptions and Behavior in the Age of Surveillance Capitalism (Doctoral dissertation, Capella University).
(16) Sindermann, C., Kuss, D. J., Throuvala, M. A., Griffiths, M. D., & Montag, C. (2020). Should we pay for our social media/messenger applications? Preliminary data on the acceptance of an alternative to the current prevailing data business model. Frontiers in Psychology, 11, 1415.
(17) Andrew, J., Baker, M., & Huang, C. (2021). Data breaches in the age of surveillance capitalism: do disclosures have a new role to play?. Critical Perspectives on Accounting, 102396.
(18) صلاح الدين النشار، غادة. (2018). إدارة الخصوصية عبر مواقع التواصل الاجتماعي بالتطبيق على موقع فيسبوك. المجلة العلمية لبحوث الإذاعة والتلفزيون، 2018(14)، 271- 335.
(19) إبراهيم السمان، هاني. (2022). اتجاهات الشباب الجامعي نحو انتهاك الحياة الخاصة عبر شبكات التواصل الاجتماعي وآليات حماية الخصوصية. مجلة البحوث والدراسات الإعلامية، 20(20)، 1- 77.
(20) أحمد محمد طه، هدير. (2022). إدارة المرأة المصرية لخصوصيتها على موقع التواصل الاجتماعي فيسبوك. مجلة البحوث والدراسات الإعلامية، 20(20)، 1- 72.
(21) سعد جودة إبراهيم، سالي. (2021). مواقع التواصل الاجتماعي وانتهاكات الخصوصية: السناب شات/ الفيس بوك نموذجًا. مجلة البحوث والدراسات الإعلامية، 18(18)، 1- 81.
(22) أحمد غريب، سحر. (2021). إدراك الجمهور لانتهاكات الخصوصية الرقمية عبر الإعلام الجديد في ضوء تأثير الشخص الثالث. مجلة البحوث والدراسات الإعلامية، 18(18)، 1- 69.
(23) حسن زيدان، سليمة. (2022). تداول المعلومات الشخصية على وسائل التواصل الاجتماعي.. الحدود والاختراقات صفحات المرأة على الفيس بوك نموذجًا. مجلة البحوث والدراسات الإعلامية، 21(21)، 1- 19.

(24) بخيت، مها مصطفى، طلبة، هناء عكاشة. (2022). مخاطر انتهاك الخصوصية للشباب المصري في إطار نموذج تأثرية الآخرين. المجلة المصرية لبحوث الرأي العام، 21(4)، 619- 673.
(25) محمود محمد محمد، مهني. (2022). استخدام التسويق الإلكتروني لتطبيقات تكنولوجيا الذكاء الاصطناعي وتحليل البيانات الضخمة وتأثيره على الخصوصية في العصر الرقمي. مجلة مستقبل العلوم الاجتماعية، 8(3)، 205- 264.
(26) البرادعي، مها عبد الحميد محمد. (2022). انتهاك خصوصية مستخدمي التطبيقات التسويقية في إطار نظرية تأثيرية الآخرين. مجلة البحوث والدراسات الإعلامية، 22(22)، 493- 578.
(27) Hinds, J., & Joinson, A. N. (2018). What demographic attributes do our digital footprints reveal? A systematic review. PloS one, 13(11), e0207112.
(28) Pew Research Center, The Digital Footprint of Europe's Refugees, 2017, Retrieved from: www.pewglobal.org/2017/06/08/digital-footprint-of-europes-refugees/. Date: 2-4-2023.
(29) Hilbert, M., Vásquez, J., Halpern, D., Valenzuela, S., & Arriagada, E. (2017). One step, two step, network step? Complementary perspectives on communication flows in Twittered citizen protests. Social science computer review, 35(4), 444-461.
(30) Robards, B., Lyall, B., & Moran, C. (2021). Confessional data selfies and intimate digital traces. New Media & Society, 23(9), 2616-2633.
(31) Wang, X., Fang, Z., & Guo, X. (2016). Tracking the digital footprints to scholarly articles from social media. Scientometrics, 109, 1365-1376.
(32) Wang, X., Xu, S., & Fang, Z. (2016). Tracing digital footprints to academic articles: An investigation of PeerJ publication referral data. arXiv preprint arXiv:1601.05271.
(33) Lambiotte, R., & Kosinski, M. (2014). Tracking the digital footprints of personality. Proceedings of the IEEE, 102(12), 1934-1939.
(34) Önder, I., Koerbitz, W., & Hubmann-Haidvogel, A. (2016). Tracing tourists by their digital footprints: The case of Austria. Journal of Travel Research, 55(5), 566-573.
(35) Girardin, F., Calabrese, F., Dal Fiore, F., Ratti, C., & Blat, J. (2008). Digital footprinting: Uncovering tourists with user-generated content. IEEE Pervasive computing, 7(4), 36-43.
(36) Golder, S. A., & Macy, M. W. (2014). Digital footprints: Opportunities and challenges for online social research. Annual Review of Sociology, 40, 129-152. P. 141.
(37) جودة، هبة (٢٠٢٢). الحماية القانونية للخصوصية الرقمية في الدول العربية. مجلة البحوث والدراسات الإعلامية، 20(20)، 1- 94.
(38) عائشة، غزيل (٢٠٢٣). الحماية الدولية للحق في الخصوصية في المجال الرقمي. مجلة المعيار، 27(4)، 404- 427.
(39) عشري برعي، أسماء. (2022). اتجاهات النخب نحو تشريعات حماية البيانات عبر مواقع التواصل الاجتماعي ودورها في حماية الخصوصية الرقمية لهم. مجلة البحوث والدراسات الإعلامية، 20(20)، 1- 68.

(40) Stainforth, E. (2022). Collective memory or the right to be forgotten? Cultures of digital memory and forgetting in the European Union. Memory Studies, 15(2), 257-270.
(41) Grimm, C., & Chiasson, S. (2014, February). Survey on the fate of digital footprints after death. In Workshop on Usable Security (USEC), Internet Society.
(42) Bunn, A. (2019). Children and the 'Right to be Forgotten': what the right to erasure means for European children, and why Australian children should be afforded a similar right. Media International Australia, 170(1), 37-46.
(43) Mitrou, L., & Karyda, M. (2012, February). EU's data protection reform and the right to be forgotten: A legal response to a technological challenge?. In 5th International Conference of Information Law and Ethics (pp. 29-30).
(44) Koops, B. J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice. SCRIPTed, 8, 229. P. 230a.
(45) Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. Suny Press. P. 1
(46) CPM Developed Glossary of Terms, Communication Privacy Management Center, Retrieved from: https://cpmcenter.iupui.edu/Teach/Glossary, Date: 17 of September 2023.
(47) Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. Op. Cit. P. 9-10. And, Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation?. Journal of family theory & review, 2(3), 175-196.
(48) Hollenbaugh, E. E. (2019). Privacy management among social media natives: An exploratory study of Facebook and Snapchat. Social Media+ Society, 5(3), 2056305119855144.
(49) Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation?. Op. Cit.
(50) Hollenbaugh, E. E. (2019). Privacy management among social media natives: An exploratory study of Facebook and Snapchat. Op. Cit.
(51) Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation?. Journal of family theory & review, 2(3), 175-196. Op. Cit.
(52) Petronio, S. (2013). Brief status report on communication privacy management theory. Journal of Family Communication, 13(1), 6-14.
(53) Metzger, M. J. (2007). Communication privacy management in electronic commerce. Journal of Computer-Mediated Communication, 12(2), 335-361.
(54) Thompson, S. K. (2012). Sampling (Vol. 755). John Wiley & Sons. P. 54.

(55) أسماء المُحكِّمين مرتبة هجائيًا:
أ. د. حلمي محسب، عميد كلية الإعلام، جامعة جنوب الوادي.
أ. د. شريف درويش اللبان، أستاذ الصحافة وتكنولوجيا الاتصال، كلية الإعلام جامعة القاهرة.
أ. د. محرز غالي، أستاذ الصحافة، كلية الإعلام جامعة القاهرة.

(56) Thatcher, J. (2014). Big data, big questions| Living on fumes: Digital footprints, data fumes, and the limitations of spatial big data. International Journal of Communication, 8, 19.
(57) Ward, C., Ellis, D., D'Ambrosio, L. A., & Coughlin, J. F. (2018). Digital breadcrumbs: A lack of data privacy and what people are doing about it. In Human-Computer Interaction. Theories, Methods, and Human Issues: 20th International Conference, HCI International 2018, Las Vegas, NV, USA, July 15–20, 2018, Proceedings, Part I 20 (pp. 599-612). Springer International Publishing. P. 605.
(58) Önder, I., Koerbitz, W., & Hubmann- Haidvogel, A. (2016). Tracing tourists by their digital footprints: The case of Austria. Op. Cit.
(59) Van Baalen, S. (2018). 'Google wants to know your location': The ethical challenges of fieldwork in the digital age. Research Ethics, 14(4), 1-17.
(60) Hinds, J., & Joinson, A. N. (2018). What demographic attributes do our digital footprints reveal? Op. Cit.
(61) Oxley, C. (2011). Digital citizenship: Developing an ethical and responsible online culture. Access, 25(3), 5-9.
(62) Mayda, M. (2022). Digital Footprint Management In Dıigital Visual Culture. Erciyes İletişim Dergisi, 9(2), 1031-1044. And Önder, I., Koerbitz, W., & Hubmann-Haidvogel, A. (2016). Tracing tourists by their digital footprints: The case of Austria. Op. Cit.
(63) Comunello, F., Martire, F., & Sabetta, L. (2022). Brushing Society Against the Grain: Digital Footprints, Scraps, Non-Human Acts, Crumbs, and Other Traces. American Behavioral Scientist, 00027642221144844.
(64) Mayda, M. (2022). Digital Footprint Management In Dıigital Visual Culture. Erciyes İletişim Dergisi, 9(2), 1031-1044.
(65) Comunello, F., Martire, F., & Sabetta, L. (2022). Brushing Society Against the Grain: Digital Footprints, Scraps, Non-Human Acts, Crumbs, and Other Traces. Op. Cit.
(66) Koops, B. J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice. Op. Cit. Also see: Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). Digital Footprints. PEW Internet & American Life Project. Pew Internet & American life project, December.
(67) Hengstler, J. (2011). Managing your digital footprint: Ostriches v. Eagles. Education for a digital world, 2, 89-139.
(68) Alhamami, F. M. A. (2020). Digital Footprints of University Students (Doctoral dissertation, Flinders University, College of Science and Engineering.).
(69) Büchi, M., Lutz, C., & Micheli, M. (2017, May). Life online: The digital footprint gap. In International scientific conference for the Partnership for Progress on the Digital Divide. Also see: Büchi, M. (2017). Digital inequalities: Differentiated Internet use and social implications (Doctoral dissertation, University

of Zurich). Also see: Robinson, L., Cotten, S. R., Ono, H., Quan-Haase, A., Mesch, G., Chen, W., ... & Stern, M. J. (2015). Digital inequalities and why they matter. Information, communication & society, 18(5), 569-582.
(70) Arakerimath, A., & Gupta, P. K. (2015). Digital footprint: Pros, cons, and future. International Journal of Latest Technology in Engineering, 4(10), 52-56.
(71) Sjöberg, M., Chen, H. H., Floréen, P., Koskela, M., Kuikkaniemi, K., Lehtiniemi, T., & Peltonen, J. (2017). Digital me: Controlling and making sense of my digital footprint. In Symbiotic Interaction: 5th International Workshop, Symbiotic 2016, Padua, Italy, September 29–30, 2016, Revised Selected Papers 5 (pp. 155-167). Springer International Publishing.
(72) Denise Seguin, What Does Your Digital Footprint Say About You?, Retrieved from: https://paradigmeducation.com/2016/12/30/digital-footprint-say/. Date: 3-12-2021
(73) Natasha Singer (2013) They Loved Your G.P.A. Then They Saw Your Tweets. Retrieved from: www.nytimes.com/2013/11/10/business/they-loved-your-gpa-then-they-saw-your-tweets.html. at: 5-3-2023.
(74) Beal, A., & Strauss, J. (2009). Radically transparent: Monitoring and managing reputations online. John Wiley & Sons. P. 111.
(75) Mitrou, L., & Karyda, M. (2012, February). EU's data protection reform and the right to be forgotten: A legal response to a technological challenge?. In 5th International Conference of Information Law and Ethics (pp. 29-30).
(76) Esposito, E. (2017). Algorithmic memory and the right to be forgotten on the web. Big Data & Society, 4(1), 2053951717703996.
(77) No, R. (1999). Rec (99) 5 of the Committee of Ministers to member states on the protection of privacy on the Internet (adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers' Deputies). Council of Europe.
(78) General Data Protection Regulation. Retrieved from: https://gdpr-info.eu. Date: 12-3-2023.
(79) Squires, J. (2014). Google Spain SL v Agencia Espanola de Proteccion de Datos (European Court of Justice, C-131/12, 13 May 2014). Adelaide Law Review, The, 35(2), 463-471.
(80) محمود محمد محمد، مهني. (2022). استخدام التسويق الإلكتروني لتطبيقات تكنولوجيا الذكاء الاصطناعي وتحليل البيانات الضخمة وتأثيره على الخصوصية في العصر الرقمي. مرجع سابق.
(81) أحمد غريب، سحر. (2021). إدراك الجمهور لانتهاكات الخصوصية الرقمية عبر الإعلام الجديد في ضوء تأثير الشخص الثالث. مرجع سابق.
(82) Michael, M., & Lupton, D. (2017). 'Depends on who's got the data': public understandings of personal digital dataveillance. Op. Cit.
(83) Marinelli, A., & Parisi, S. (2022). Apps, Platforms, and Everyday Practices: How People Perceive and Care (or not) About the Digital Traces They Leave Online. OP. Cit.

(84) Metzger, M. J. (2007). Communication privacy management in electronic commerce. Op. Cit.

(85) محمـود محمـد محمـد، مهنـي. (2022). اسـتخدام التسـويق الإلكترونـي لتطبيقـات تكنولوجيـا الـذكاء الاصطناعي وتحليل البيانات الضخمة وتأثيره على الخصوصية في العصر الرقمي. مرجع سابق.

(86) البرادعي، مها عبد الحميد محمد. (2022). انتهاك خصوصية مستخدمي التطبيقات التسويقية في إطار نظرية تأثيرية الآخرين. مرجع سابق.

(87) أحمد غريب، سحر. (2021). إدراك الجمهور لانتهاكات الخصوصية الرقمية عبر الإعلام الجديد في ضوء تأثير الشخص الثالث. مرجع سابق.

(88) سعد جودة إبراهيم، سالي. (2021). مواقع التواصل الاجتماعي وانتهاكات الخصوصية: السناب شات/ الفيس بوك نموذجًا. مرجع سابق.

(89) محمـود محمـد محمـد، مهنـي. (2022). اسـتخدام التسـويق الإلكترونـي لتطبيقـات تكنولوجيـا الـذكاء الاصطناعي وتحليل البيانات الضخمة وتأثيره على الخصوصية في العصر الرقمي. مرجع سابق.

(90)صلاح الدين النشار، غادة. (2018). إدارة الخصوصية عبر مواقع التواصل الاجتماعي بالتطبيق على موقع فيسبوك. مرجع سابق.

**References:**


- Tomasello, F. (2023). From industrial to digital citizenship: rethinking social rights in cyberspace. Theory and society, 52(3), 463-486.
- Montag, C., Lachmann, B., Herrlich, M., & Zweig, K. (2019). Addictive features of social media/messenger platforms and freemium games against the background of psychological and economic theories. International journal of environmental research and public health, 16(14), 2612.
- Council of Europe (2014). Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users. (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies)
- Buchanan, R., Southgate, E., & Smith, S. P. (2019). 'The whole world's watching really': Parental and educator perspectives on managing children's digital lives. Global Studies of Childhood, 9(2), 167-180.
- Chalklen, C., & Anderson, H. (2017). Mothering on Facebook: Exploring the privacy/openness paradox. Social Media+ Society, 3(2), 2056305117707187.
- Buchanan, R., Southgate, E., Smith, S. P., Murray, T., & Noble, B. (2017). Post no photos, leave no trace: Children's digital footprint management strategies. E-learning and digital Media, 14(5), 275-290.
- Marinelli, A., & Parisi, S. (2022). Apps, Platforms, and Everyday Practices: How People Perceive and Care (or not) About the Digital Traces They Leave Online. American Behavioral Scientist, 00027642221144852.
- The Australian Communications and Media Authority, Digital Footprints and Identities, Retrieved from: www.acma.gov.au/theACMA/Library/researchacma. Date: 12-10-2020.
- Camacho, M., Minelli, J., & Grosseck, G. (2012). Self and identity: raising undergraduate students' awareness on their digital footprints. Procedia-Social and Behavioral Sciences, 46, 3176-3181.
- Holloway, D. (2019). Surveillance capitalism and children's data: the Internet of toys and things for children. Media International Australia, 170(1), 27-36..
- Montag, C., & Elhai, J. D. (2023). On Social Media Design,(Online-) Time Well-spent and Addictive Behaviors in the Age of Surveillance Capitalism. Current Addiction Reports, 1-7.
- Michael, M., & Lupton, D. (2017). 'Depends on who's got the data': public understandings of personal digital dataveillance.
- Di Bene, E. (2022). Online Privacy: a Qualitative Inquiry About Privacy Perceptions and Behavior in the Age of Surveillance Capitalism (Doctoral dissertation, Capella University).
- Sindermann, C., Kuss, D. J., Throuvala, M. A., Griffiths, M. D., & Montag, C. (2020). Should we pay for our social media/messenger applications?

Preliminary data on the acceptance of an alternative to the current prevailing data business model. Frontiers in Psychology, 11, 1415.
- Andrew, J., Baker, M., & Huang, C. (2021). Data breaches in the age of surveillance capitalism: do disclosures have a new role to play?. Critical Perspectives on Accounting, 102396.
- Salah aldiyn alnashar, ghadati. (2018). 'iidarat alkhususiat eabr mawaqie altawasul alaijtimaeaa bialtatbiq ealaa mawqie fisbuk. almajalat aleilmiat libuhuth al'iidhaeat waltilfizyuni, 2018(14), 271-335.
- Ibrahim alsaman, hani. (2022). yatbae alshabab aljamieia nahw antihak alhayaat alkhasat eabr shabakat altawasul aliajtimaeii waliaat alkhususiati. majalat alakhir waldirasat almanshurati, 20(20), 1-77.
- Ahmad muhamad tah, hudir. (2022). 'iidarat almar'at almisriat likhususiatiha ealaa mawqie altawasul aliajtimaeii fisbuk. majalat 'ahdath waldirasat almanshurata, 20(20), 1-72.
- Saed judih 'iibrahim, sali. (2021). mawaqie altawasul alaijtimaeii waintihakat alkhususiati: namudhaj alsanab shat/alfis buk. majalat 'ahdath waldirasat almanshurati, 18(18), 1-81.
- Ahmad ghurib, sahr. (2021). 'iidrak aljumhur liaintihakat alkhususiat alraqamiat eabr al'iielam aljadid fi daw' tathir alshakhs althaalithi. majalat 'ahdath waldirasat almanshurata, 18(18), 1-69.
- Hasan zidan, salimata. (2022). taemim almaelumat alshakhsiat ealaa wasayil altawasul alaijtimaeii. alhudud waikhtiraqat safahat almar'at ealaa alfis buk nmwdhjaan. majalat alakhir waldirasat almanshurati, 21(21), 1-19.
- Bakhayt, maha mustafi, talabahu, hana' eakashihi. (2022). qam bitanfidh al'ahdaf almisriat fi 'iitar namudhajiin yata'athar bialakhrin. almajalat almisriat libuhuth alraay aleama, 21(4), 619-673..
- Mahmud muhamad muhamad, alniqabatu. (2022). astikhdam altaswiq al'iiliktrunii litatbiqat tiknulujia aldhaka' alaistinaeii watahlil albayanat alraqmiat bikamiyaat kabirat ealaa alkhususiat fi aleasra. majalat mustaqbal aleulum alaijtimaeiati, 8(3), 205-264.
- Albaradiei, maha eabd muhamad alhamidi. (2022). tahdif 'iilaa khususiat almustakhdimin altatbiqat altaswiqiat fi 'iitar nazar litathir alakhrin. majalat alakhir waldirasat almanshurati, 22(22), 493-578.
- Hinds, J., & Joinson, A. N. (2018). What demographic attributes do our digital footprints reveal? A systematic review. PloS one, 13(11), e0207112.
- Pew Research Center, The Digital Footprint of Europe’s Refugees, 2017, Available at: www.pewglobal.org/2017/06/08/digital-footprint-of-europes-refugees/.
- Hilbert, M., Vásquez, J., Halpern, D., Valenzuela, S., & Arriagada, E. (2017). One step, two step, network step? Complementary perspectives on communication flows in Twittered citizen protests. Social science computer review, 35(4), 444-461.

- Robards, B., Lyall, B., & Moran, C. (2021). Confessional data selfies and intimate digital traces. New Media & Society, 23(9), 2616-2633.
- Wang, X., Fang, Z., & Guo, X. (2016). Tracking the digital footprints to scholarly articles from social media. Scientometrics, 109, 1365-1376..
- Wang, X., Xu, S., & Fang, Z. (2016). Tracing digital footprints to academic articles: An investigation of PeerJ publication referral data. arXiv preprint arXiv:1601.05271.
- Lambiotte, R., & Kosinski, M. (2014). Tracking the digital footprints of personality. Proceedings of the IEEE, 102(12), 1934-1939.
- Önder, I., Koerbitz, W., & Hubmann-Haidvogel, A. (2016). Tracing tourists by their digital footprints: The case of Austria. Journal of Travel Research, 55(5), 566-573.
- Girardin, F., Calabrese, F., Dal Fiore, F., Ratti, C., & Blat, J. (2008). Digital footprinting: Uncovering tourists with user-generated content. IEEE Pervasive computing, 7(4), 36-43.
- Golder, S. A., & Macy, M. W. (2014). Digital footprints: Opportunities and challenges for online social research. Annual Review of Sociology, 40, 129-152. P. 141.
- Heba Goda, alhimayat alqanuniat lilkhususiat alraqamiat fi alduwal alearabiati. majalat 'ahdath waldirasat almanshurati, 20(20), 1-94.
- Eayishati, ghazil (2023). alhimayat aldawliat lihaqi alkhususiat fi almajal alraqmay. majalat aksi, 27(4), 404-427.
- Ashri barae, 'asma'. (2022). aitijahat alnukhab nahw himayat albayanat eabr mawaqie altawasul wadawriha fi himayat alkhususiat alraqamiat lahum. majalat 'ahdath waldirasat almanshurata, 20(20), 1-68.
- Stainforth, E. (2022). Collective memory or the right to be forgotten? Cultures of digital memory and forgetting in the European Union. Memory Studies, 15(2), 257-270.
- Grimm, C., & Chiasson, S. (2014, February). Survey on the fate of digital footprints after death. In Workshop on Usable Security (USEC), Internet Society.
- Bunn, A. (2019). Children and the ‘Right to be Forgotten’: what the right to erasure means for European children, and why Australian children should be afforded a similar right. Media International Australia, 170(1), 37-46.
- Mitrou, L., & Karyda, M. (2012, February). EU's data protection reform and the right to be forgotten: A legal response to a technological challenge?. In 5th International Conference of Information Law and Ethics (pp. 29-30)..
- Koops, B. J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the right to be forgotten in big data practice. SCRIPTed, 8, 229. P. 230a.
- Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. Suny Press. P. 1

- CPM Developed Glossary of Terms, Communication Privacy Management Center, Retrieved from: https://cpmcenter.iupui.edu/Teach/Glossary, Date: 17 of September 2023.
- Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation?. Journal of family theory & review, 2(3), 175-196.
- Hollenbaugh, E. E. (2019). Privacy management among social media natives: An exploratory study of Facebook and Snapchat. Social Media+ Society, 5(3), 2056305119855144.
- Petronio, S. (2013). Brief status report on communication privacy management theory. Journal of Family Communication, 13(1), 6-14.
- Metzger, M. J. (2007). Communication privacy management in electronic commerce. Journal of Computer-Mediated Communication, 12(2), 335-361.
- Thompson, S. K. (2012). Sampling (Vol. 755). John Wiley & Sons. P. 54.
- Thatcher, J. (2014). Big data, big questions| Living on fumes: Digital footprints, data fumes, and the limitations of spatial big data. International Journal of Communication, 8, 19.
- Ward, C., Ellis, D., D'Ambrosio, L. A., & Coughlin, J. F. (2018). Digital breadcrumbs: A lack of data privacy and what people are doing about it. In Human-Computer Interaction. Theories, Methods, and Human Issues: 20th International Conference, HCI International 2018, Las Vegas, NV, USA, July 15–20, 2018, Proceedings, Part I 20 (pp. 599-612). Springer International Publishing. P. 605.
- Van Baalen, S. (2018). 'Google wants to know your location': The ethical challenges of fieldwork in the digital age. Research Ethics, 14(4), 1-17.
- Oxley, C. (2011). Digital citizenship: Developing an ethical and responsible online culture. Access, 25(3), 5-9.
- Mayda, M. (2022). Digital Footprint Management In Dıigital Visual Culture. Erciyes İletişim Dergisi, 9(2), 1031-1044
- Comunello, F., Martire, F., & Sabetta, L. (2022). Brushing Society Against the Grain: Digital Footprints, Scraps, Non-Human Acts, Crumbs, and Other Traces. American Behavioral Scientist, 00027642221144844.
- Mayda, M. (2022). Digital Footprint Management In Dıigital Visual Culture. Erciyes İletişim Dergisi, 9(2), 1031-1044.
- Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). Digital Footprints. PEW Internet & American Life Project. Pew Internet & American life project, December./
- Hengstler, J. (2011). Managing your digital footprint: Ostriches v. Eagles. Education for a digital world, 2, 89-139.
- Alhamami, F. M. A. (2020). Digital Footprints of University Students (Doctoral dissertation, Flinders University, College of Science and Engineering.).

- Büchi, M., Lutz, C., & Micheli, M. (2017, May). Life online: The digital footprint gap. In International scientific conference for the Partnership for Progress on the Digital Divide. Also see: Büchi, M. (2017). Digital inequalities: Differentiated Internet use and social implications (Doctoral dissertation, University of Zurich). Also see: Robinson, L., Cotten, S. R., Ono, H., Quan-Haase, A., Mesch, G., Chen, W., ... & Stern, M. J. (2015). Digital inequalities and why they matter. Information, communication & society, 18(5), 569-582.
- Arakerimath, A., & Gupta, P. K. (2015). Digital footprint: Pros, cons, and future. International Journal of Latest Technology in Engineering, 4(10), 52-56.
- Sjöberg, M., Chen, H. H., Floréen, P., Koskela, M., Kuikkaniemi, K., Lehtiniemi, T., & Peltonen, J. (2017). Digital me: Controlling and making sense of my digital footprint. In Symbiotic Interaction: 5th International Workshop, Symbiotic 2016, Padua, Italy, September 29–30, 2016, Revised Selected Papers 5 (pp. 155-167). Springer International Publishing.
- Denise Seguin, What Does Your Digital Footprint Say About You?, Retrieved from: https://paradigmeducation.com/2016/12/30/digital-footprint-say/. Date: 3-12-2021
- Natasha Singer (2013) They Loved Your G.P.A. Then They Saw Your Tweets. Retrieved from: www.nytimes.com/2013/11/10/business/they-loved-your-gpa-then-they-saw-your-tweets.html.
- Beal, A., & Strauss, J. (2009). Radically transparent: Monitoring and managing reputations online. John Wiley & Sons. P. 111.
- Mitrou, L., & Karyda, M. (2012, February). EU's data protection reform and the right to be forgotten: A legal response to a technological challenge?. In 5th International Conference of Information Law and Ethics (pp. 29-30).
- Esposito, E. (2017). Algorithmic memory and the right to be forgotten on the web. Big Data & Society, 4(1), 2053951717703996.
- No, R. (1999). Rec (99) 5 of the Committee of Ministers to member states on the protection of privacy on the Internet (adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers' Deputies). Council of Europe.
- General Data Protection Regulation. Retrieved from: https://gdpr-info.eu. Date: 12-12-2023.
- Squires, J. (2014). Google Spain SL v Agencia Espanola de Proteccion de Datos (European Court of Justice, C-131/12, 13 May 2014). Adelaide Law Review, The, 35(2), 463-471.

# Journal of Mass Communication Research «J M C R»

**A scientific journal issued by Al-Azhar University, Faculty of Mass Communication**





**Correspondences**

- Al-Azhar University- Faculty of Mass Communication.
- Telephone Number: 0225108256
- Our website: http://jsb.journals.ekb.eg
- E-mail: mediajournal2020@azhar.edu.eg



**Issue 69 January 2024 - part 1**

**Deposit - registration number at Darelkotob almasrya /6555**

**International Standard Book Number "Electronic Edition" 2682- 292X**

**International Standard Book Number «Paper Edition»9297- 1110**

# Rules of Publishing

**Our Journal Publishes Researches, Studies, Book Reviews, Reports, and Translations according to these rules:**

- Publication is subject to approval by two specialized referees.
- The Journal accepts only original work; it shouldn't be previously published before in a refereed scientific journal or a scientific conference.
- The length of submitted papers shouldn't be less than 5000 words and shouldn't exceed 10000 words. In the case of excess the researcher should pay the cost of publishing.
- Research Title whether main or major, shouldn't exceed 20 words.
- Submitted papers should be accompanied by two abstracts in Arabic and English. Abstract shouldn't exceed 250 words.
- Authors should provide our journal with 3 copies of their papers together with the computer diskette. The Name of the author and the title of his paper should be written on a separate page. Footnotes and references should be numbered and included in the end of the text.
- Manuscripts which are accepted for publication are not returned to authors. It is a condition of publication in the journal the authors assign copyrights to the journal. It is prohibited to republish any material included in the journal without prior written permission from the editor.
- Papers are published according to the priority of their acceptance.
- Manuscripts which are not accepted for publication are returned to authors.